Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004852

International filing date: 11 March 2005 (11.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-074739
Filing date: 16 March 2004 (16.03.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/004852

日　本　国　特　許　庁
JAPAN PATENT OFFICE

11.3.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　２００４年　３月１６日

出願番号
Application Number:　特願２００４－０７４７３９

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is　ＪＰ２００４－０７４７３９

出願人
Applicant(s):　松下電器産業株式会社

２００５年　４月１５日

特許庁長官
Commissioner,
Japan Patent Office　小川　洋

出証番号　出証特２００５－３０３４１２４

【書類名】　特許願
【整理番号】　2048150045
【提出日】　平成16年 3月16日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、
秘密鍵を生成する秘密鍵生成手段と、
前記条件を特定するパラメータを複数取得するパラメータ取得手段と、
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と
を備えることを特徴とする情報セキュリティ装置。
【請求項２】
前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、
前記パラメータ取得手段は、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、
前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成する
ことを特徴とする請求項１に記載の情報セキュリティ装置。
【請求項３】
前記情報セキュリティ装置は、更に、
前記公開鍵生成手段により生成された前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信する公開鍵送信手段と、
前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得する公開鍵証明書取得手段と、
前記秘密鍵生成手段により生成された秘密鍵、及び、前記公開鍵証明書取得手段により取得された複数の公開鍵証明書を記憶する鍵記憶手段と
を備えることを特徴とする請求項２に記載の情報セキュリティ装置。
【請求項４】
前記情報セキュリティ装置は、更に、
前記鍵記憶手段から一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公開鍵証明書の発行元であるサーバ装置へ送信するコンテンツ要求手段と、
前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するコンテンツ取得手段と
を備えることを特徴とする請求項３に記載の情報セキュリティ装置。
【請求項５】
前記コンテンツ取得手段は、
前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証する認証部と、
前記認証部による認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有する鍵共有部と、
前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信する受信部と、
受信した暗号化コンテンツを前記鍵情報を用いて復号する復号部と
を備えることを特徴とする請求項４に記載の情報セキュリティ装置。
【請求項６】
前記鍵記憶手段は、当該情報セキュリティ装置に挿入された可搬型のメモリカードであって、
前記公開鍵生成手段は、前記メモリカードに前記秘密鍵及び前記複数の公開鍵証明書を書き込み、
前記メモリカードは、外部から解読及び改竄が不可能なセキュアな記憶領域を含み、前

記セキュアな記憶領域に前記秘密鍵を格納する
　ことを特徴とする請求項３に記載の情報セキュリティ装置。
【請求項７】
　前記情報セキュリティ装置は、更に、
　前記メモリカードが当該情報セキュリティ装置に挿入されると、前記メモリカードの正当性を認証するメモリカード認証手段と、
　前記メモリカード認証手段による認証に失敗した場合、前記公開鍵生成手段による前記秘密鍵及び前記複数の公開鍵証明書の前記メモリカードへの書き込みを抑制する書込抑制手段と
　を備えることを特徴とする請求項６に記載の情報セキュリティ装置。
【請求項８】
　前記情報セキュリティ装置は、楕円曲線上の離散対数問題を安全性の根拠とし、
　前記パラメータ取得手段は、楕円曲線を構成するパラメータを複数取得し、
　前記公開鍵生成手段は、取得した複数のパラメータごとに、前記秘密鍵に楕円曲線上の乗算を施すことにより、前記複数の公開鍵を生成する
　ことを特徴とする請求項１に記載の情報セキュリティ装置。
【請求項９】
　前記秘密鍵生成手段は、１個の秘密鍵ＳＫを生成し、
　前記パラメータ取得手段は、楕円曲線$y^2 = x^3 + ax + b$を構成するパラメータａ、ｂ、素数ｐ、及び前記楕円曲線上の元Ｇの組を複数取得し、
　前記公開鍵生成手段は、取得した複数の組ごとに、ＳＫ＊Ｇ（ｍｏｄｐ）を計算することにより、前記複数の公開鍵を生成する
　ことを特徴とする請求項８に記載の情報セキュリティ装置。
【請求項１０】
　前記情報セキュリティ装置は、ＲＳＡ暗号を安全性の根拠とし、
　前記秘密鍵生成手段は、１個の秘密鍵ｄを生成し、
　前記パラメータ取得手段は、前記パラメータとして、素数の組（Ｐ、Ｑ）を複数取得し、
　前記公開鍵生成手段は、取得した複数の素数の組ごとに、
　Ｎ＝ＰＱを計算し、更に、$ed \equiv 1 \bmod (P-1)(Q-1)$から、ｅを計算し、前記複数の公開鍵（Ｎ、ｅ）の組を生成する
　ことを特徴とする請求項１に記載の情報セキュリティ装置。
【請求項１１】
　同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱うメモリカードであって、
　秘密鍵を生成する秘密鍵生成手段と、
　前記条件を特定するパラメータを複数取得するパラメータ取得手段と、
　取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と、
　前記秘密鍵を、外部から解読及び改竄が不可能なセキュアな領域に記憶する秘密鍵記憶手段と
　を備えることを特徴とするメモリカード。
【請求項１２】
　前記メモリカードは、ネットワークを介して複数のサーバ装置と接続された端末に挿入されており、
　前記パラメータ取得手段は、前記端末を介して、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、
　前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成する
　ことを特徴とする請求項１１に記載のメモリカード。

【請求項１３】
前記メモリカードは、更に、
前記秘密鍵及び前記複数の公開鍵を用いて、前記端末を介して、前記複数のサーバ装置それぞれから、安全かつ確実にコンテンツを取得する
ことを特徴とする請求項１２に記載のメモリカード。
【請求項１４】
同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティシステムであって、
秘密鍵を生成する秘密鍵生成手段と、
前記条件を特定するパラメータを複数個取得するパラメータ取得手段と、
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と
を備えることを特徴とする情報セキュリティシステム。
【請求項１５】
同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置で用いられる鍵生成方法であって、
秘密鍵を生成する秘密鍵生成ステップと、
前記条件を特定するパラメータを複数取得するパラメータ取得ステップと、
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成ステップと
を含むことを特徴とする鍵生成方法。
【請求項１６】
同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置で用いられる鍵生成プログラムであって、
秘密鍵を生成する秘密鍵生成ステップと、
前記条件を特定するパラメータを複数取得するパラメータ取得ステップと、
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成ステップと
を含むことを特徴とする鍵生成プログラム。

【書類名】明細書
【発明の名称】情報セキュリティ装置及び情報セキュリティシステム
【技術分野】
【０００１】
本発明は、安全かつ確実にコンテンツを送受信する技術に関する。
【背景技術】
【０００２】
端末がコンテンツ配信業者のサービスを利用する場合、端末と、コンテンツ配信業者が有するサーバ装置とは、相互認証を行い、相互認証が成功した場合に安全に鍵を共有することにより安全な通信路、所謂ＳＡＣ（Secure　Authentication　Channel）を確立し、ＳＡＣを介してコンテンツを送受信する技術が特許文献１に開示されている。
【特許文献１】特開平１１－２３４２５９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
近年、コンテンツ配信サービスを提供する業者が増加してきており、１台の端末で複数業者のサービスを利用する場合に対応できるシステムが要望されている。
そこで本発明は、１台の端末で複数業者のサービスを利用するのに適した情報セキュリティ装置及び情報セキュリティシステムを提供することを目的とする。
【課題を解決するための手段】
【０００４】
上記の目的を達成するために、本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段とを備えることを特徴とする。
【０００５】
また、前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、前記パラメータ取得手段は、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成することを特徴とする。
また、前記情報セキュリティ装置は、更に、前記公開鍵生成手段により生成された前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信する公開鍵送信手段と、前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得する公開鍵証明書取得手段と、前記秘密鍵生成手段により生成された秘密鍵、及び、前記公開鍵証明書取得手段により取得された複数の公開鍵証明書を記憶する鍵記憶手段とを備えることを特徴とする
また、前記情報セキュリティ装置は、更に、前記鍵記憶手段から一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公開鍵証明書の発行元であるサーバ装置へ送信するコンテンツ要求手段と、前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するコンテンツ取得手段とを備えることを特徴とする。
【０００６】
また、前記コンテンツ取得手段は、前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証する認証部と、前記認証部による認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有する鍵共有部と、前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信する受信部と、受信した暗号化コンテンツを前記鍵情報を用いて復号する復号部とを備えることを特徴とする。

【０００７】
更に、上記目的を達成するための、本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱うメモリカードであって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と、前記秘密鍵を、外部から解読及び改竄が不可能なセキュアな領域に記憶する秘密鍵記憶手段とを備えることを特徴とする。
【０００８】
また、前記メモリカードは、ネットワークを介して複数のサーバ装置と接続された端末に挿入されており、前記パラメータ取得手段は、前記端末を介して、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成することを特徴とする。
【０００９】
また、前記メモリカードは、更に、前記秘密鍵及び前記複数の公開鍵を用いて、前記端末を介して、前記複数のサーバ装置それぞれから、安全かつ確実にコンテンツを取得することを特徴とする。
【発明の効果】
【００１０】
本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成し、前記条件を特定するパラメータを複数取得し、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成することを特徴とする。
【００１１】
この構成によると、情報セキュリティ装置は、秘密鍵から複数個の公開鍵を生成するため、秘密鍵と公開鍵とが１対１に対応している従来の装置と比較すると、複数個の公開鍵を生成する場合に、生成、管理する鍵の数が減るという効果がある。
ここで、前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成するように構成してもよい。
【００１２】
この構成によると、情報セキュリティ装置は、複数のサーバ装置から、それぞれ異なるパラメータを取得することで、１個の秘密鍵から、複数個の異なる公開鍵を生成することができる。そのため、従来の装置が、通信を行うサーバ装置毎に１個の秘密鍵と１個の公開鍵とのペアを生成し、管理していたのと比較し、本発明の情報セキュリティ装置は、生成、管理する鍵の数が減るという効果がある。
【００１３】
ここで、前記情報セキュリティ装置は、更に、生成した前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信し、前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得し、生成した秘密鍵、及び、取得した複数の公開鍵証明書を記憶するように構成してもよい。
この構成によると、従来の装置は、通信を行うサーバ装置毎に１個の秘密鍵と１個公開鍵とのペアを記憶していたのと比較して、本発明の情報セキュリティ装置では、鍵記憶手段が記憶する鍵の数が減るので、記憶領域が削減され、コストの節減に繋がる。
【００１４】
ここで、前記情報セキュリティ装置は、更に、記憶している複数の公開鍵証明書から、一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公

開鍵証明書の発行元であるサーバ装置へ送信し、前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するように構成してもよい。

【００１５】

この構成によると、情報セキュリティ装置は、記憶されている複数個の公開鍵証明書から、１個の公開鍵証明書を選ぶことで、１個の秘密鍵と選ばれた公開鍵証明書に含まれる公開鍵とを用いて、対応するサーバ装置からコンテンツをセキュアに取得することができる。

ここで、前記情報セキュリティ装置は、前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証し、前記認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有し、前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信し、受信した暗号化コンテンツを、前記鍵情報を用いて復号するように構成してもよい。

【００１６】

この構成によると、情報セキュリティ装置は、サーバ装置と相互認証を行い、その後、安全に鍵情報を共有することにより、サーバ装置と安全な通信路を確立することができる。

ここで、前記情報セキュリティ装置内の記憶装置は、当該情報セキュリティ装置に挿入された可搬型のメモリカードであって、前記情報セキュリティ装置は、前記メモリカードに前記秘密鍵及び前記複数の公開鍵証明書を書き込み、前記メモリカードは、外部から解読及び改竄が不可能なセキュアな記憶領域を含み、前記セキュアな記憶領域に前記秘密鍵を格納するように構成してもよい。

【００１７】

この構成によると、情報セキュリティ装置内の記憶装置は、可搬型のメモリカードにより実現される。情報セキュリティ装置は、秘密鍵をメモリカードの耐タンパーモジュールに格納することにより、秘密鍵をセキュアに保持することができる。

ここで、前記情報セキュリティ装置は、更に、記メモリカードが当該情報セキュリティ装置に挿入されると、前記メモリカードの正当性を認証し、前記認証に失敗した場合、前記秘密鍵及び前記複数の公開鍵証明書の前記メモリカードへの書き込みを抑制するように構成してもよい。

【００１８】

この構成によると、情報セキュリティ装置は、メモリカードの認証に成功した場合のみ、メモリカードに秘密鍵と公開鍵証明書とを書き込むので、不正なメモリカードに秘密鍵が書き込まれることにより秘密鍵が暴露されるのを防ぐことができる。

ここで、前記情報セキュリティ装置は、楕円曲線上の離散対数問題を安全性の根拠とし、楕円曲線を構成するパラメータを複数取得し、取得した複数のパラメータごとに、前記秘密鍵に楕円曲線上の乗算を施すことにより、前記複数の公開鍵を生成するように構成してもよい。また、前記情報セキュリティ装置は、１個の秘密鍵ＳＫを生成し、楕円曲線$y^2 = x^3 + ax + b$を構成するパラメータａ、ｂ、素数ｐ、及び前記楕円曲線上の元Ｇの組を複数取得し、取得した複数の組ごとに、ＳＫ＊Ｇ（ｍｏｄｐ）を計算することにより、前記複数の公開鍵を生成するように構成してもよい。

【００１９】

この構成によると、情報セキュリティ装置は、安全性の高い楕円曲線暗号を用いることで、安全かつ確実にコンテンツを取得することができる。

ここで、前記情報セキュリティ装置は、ＲＳＡ暗号を安全性の根拠とし、１個の秘密鍵ｄを生成し、前記パラメータとして、素数の組（Ｐ、Ｑ）を複数取得し、取得した複数の素数の組ごとに、Ｎ＝ＰＱを計算し、更に、ｅｄ≡１ｍｏｄ（Ｐ－１）（Ｑ－１）から、ｅを計算し、前記複数の公開鍵（Ｎ、ｅ）の組を生成するように構成してもよい。

【００２０】

この構成によると、情報セキュリティ装置は、公開鍵暗号方式としてＲＳＡ暗号を用いるため、本発明を、汎用のコンピュータシステムで実現することが可能である。

【発明を実施するための最良の形態】

【００２１】

本発明に係る実施の形態として、情報セキュリティシステム１について説明する。情報セキュリティシステム１は、１台の端末で複数のコンテンツ配信業者が提供するサービスを利用するシステムである。

以下では、情報セキュリティシステム１について図面を参照して説明する。

＜構成＞

図１は、情報セキュリティシステム１の構成を示すシステム構成図である。同図に示す様に、情報セキュリティシステム１は、端末１０、メモリカード２０、サーバ装置３０、サーバ装置４０及びサーバ装置５０から構成される。なお、メモリカード２０は、端末１０のメモリカードスロットに挿入して用いられ、端末１０と、サーバ装置３０、サーバ装置４０及びサーバ装置５０とは、ネットワーク６０を介して接続されている。なお、ネットワーク６０の具体例は、インターネットである。

【００２２】

端末１０及びメモリカード２０は、コンテンツ配信サービスを利用する利用者が有する装置であり、サーバ装置３０、サーバ装置４０及びサーバ装置５０は、それぞれ異なるコンテンツ配信業者が有する装置である。コンテンツ配信業者は、利用者に対して、コンテンツ配信サービスを提供する。

なお、端末１０、メモリカード２０、サーバ装置３０、サーバ装置４０及びサーバ装置５０は、コンテンツを安全かつ確実に扱う装置であるので、これらの装置を情報セキュリティ装置と呼称することもある。

【００２３】

１．端末１０

ここでは、端末１０の構成について詳細に説明する。

図２は、端末１０の構成を機能的に示す機能ブロック図である。同図に示す様に、端末１０は、通信部１０１、操作入力部１０２、制御部１０３、メモリカード入出力部１０４、メモリカード認証部１０５、ＣＲＬ格納部１０６、公開鍵暗号処理部１０７、記憶部１０８及び再生部１０９から構成される。

【００２４】

端末１０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクドライブユニット、ネットワーク接続ユニット、ＭＰＥＧデコーダ、ＭＰＥＧエンコーダ及びメモリカードスロット等から構成されるコンピュータシステムである。

（１）通信部１０１

通信部１０１は、Ｗｅｂブラウザを備えるネットワーク接続ユニットであって、ネットワーク６０を介してサーバ装置３０、サーバ装置４０及びサーバ装置５０と接続されている。

【００２５】

通信部１０１は、サーバ装置３０からネットワーク６０を介して情報を受信し、受信した情報を制御部１０３へ出力する。また、通信部１０１は、制御部１０３から情報を受け取り、受け取った情報をネットワーク６０を介してサーバ装置３０へ送信する。同様に、通信部１０１は、サーバ装置４０からネットワーク６０を介して情報を受信し、受信した情報を制御部１０３へ出力する。また、通信部１０１は、制御部１０３から情報を受け取り、受け取った情報をネットワーク６０を介してサーバ装置４０へ送信する。同様に、通信部１０１は、サーバ装置５０からネットワーク６０を介して情報を受信し、受信した情報を制御部１０３へ出力する。また、通信部１０１は、制御部１０３から情報を受け取り、受け取った情報をネットワーク６０を介してサーバ装置５０へ送信する。

【００２６】

ここで、通信部１０１が各サーバ装置へ送信する情報の具体例は、サービス加入要求、

サービス利用要求、各サーバ装置とのＳＡＣ確立に用いる署名データ、鍵情報などである。また、通信部１０１が各サーバ装置から受信する情報の具体例は、各サーバ装置とのＳＡＣ確立に用いる署名データ、鍵情報、楕円曲線のシステムパラメータ、認証及び鍵共有処理の後に各サーバ装置から送信されるコンテンツ、などである。

【００２７】

更に、通信部１０１は、ネットワーク６０を介して、認証局（以下、「ＣＡ（Certification Authority）」と呼称する）と接続されており、通信部１０１は、ＣＡとの間で以下のように情報の送受信を行う。

通信部１０１は、ＣＡから常に最新のＣＲＬ（Certification Revocation List）を受信し、受信した最新のＣＲＬを、制御部１０３を介してＣＲＬ格納部１０６に格納する。ＣＲＬについては後述する。

【００２８】

通信部１０１は、制御部１０３を介して公開鍵暗号処理部１０７から公開鍵「ＰＫ＿００１０」を受け取り、受け取った公開鍵をＣＡへ送信する。また、通信部１０１は、ＣＡから公開鍵「ＰＫ＿００１０」に対応する公開鍵証明書「Ｃｅｒｔ＿００１０」を受信し、受信した公開鍵証明書を制御部１０３へ出力する。

ここで、本明細書において、「楕円曲線のシステムパラメータ」とは、楕円曲線Ｅ：$y^2 = x^3 + ax + b$を構成するａ及びｂ、更に、素数ｐ、ｐの位数ｑ、楕円曲線Ｅ上の任意の点（ベースポイント）Ｇを指すこととする。

（２）操作入力部１０２

操作入力部１０２は、利用者からの操作を受け付けるボタンなどを備える。操作入力部１０２は、利用者からの操作を受け付け、受け付けた操作に対応する操作信号を生成し、生成した操作信号を制御部１０３へ出力する。

【００２９】

ここで、操作信号の具体例は、サービス加入要求を示す信号、サービス利用要求を示す信号などである。

（３）制御部１０３

制御部１０３は、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成され、マイクロプロセッサがコンピュータプログラムを実行することにより、制御部１０３は、以下に示す処理を行い、端末１０の全体を制御する。

【００３０】

（ａ）制御部１０３は、メモリカード入出力部１０４から、メモリカード２０の挿入を検知したことを示す信号を受け取ると、メモリカード認証部１０５に対して、メモリカード２０の認証処理を行う指示を出力する。

（ｂ）制御部１０３は、メモリカード認証部１０５から「認証ＯＫ」を示す信号を受け取ると、ＣＡから公開鍵証明書の発行を受ける。より具体的には、制御部１０３は、公開鍵暗号処理部１０７から出力される公開鍵「ＰＫ＿００１０」と予め内部に記憶している自身のデバイスＩＤ「ＩＤ＿００１０」とを、通信部１０１を介してＣＡへ送信する。制御部１０３は、通信部１０１を介して公開鍵「ＰＫ＿００１０」に対応する公開鍵証明書「Ｃｅｒｔ＿００１０」をＣＡから受信し、受信した公開鍵証明書を、メモリカード入出力部１０４を介してメモリカード２０へ出力する。

【００３１】

（ｃ）制御部１０３は、操作入力部１０２から操作信号を受け取り、受け取った操作信号に応じた処理を行う。

例えば、制御部１０３は、操作入力部１０２から、サーバ装置３０、サーバ装置４０、又はサーバ装置５０へのサービス加入要求を示す操作信号を受け取ると、メモリカード入出力部１０４に対して、メモリカード２０から公開鍵証明書「Ｃｅｒｔ＿００１０」を読み出す指示を出力し、更に、要求に対応するサーバ装置とＳＡＣを確立し、サービス加入処理を行う指示を、公開鍵暗号処理部１０７に出力する。

【００３２】

また、制御部１０３は、操作入力部１０２から、サーバ装置３０、サーバ装置４０又はサーバ装置５０へのサービス利用要求を示す操作信号を受け取ると、メモリカード入出力部１０４に対して、メモリカード２０から、サービス用秘密鍵ＳＫ及び要求に対応するサーバ装置から受け取った公開鍵証明書を読み出す指示を出力し、更に、対応するサーバ装置とＳＡＣを確立して、コンテンツを取得する指示を、公開鍵暗号処理部１０７に出力する。

【００３３】

（ｄ）また、制御部１０３は、端末１０とサーバ装置３０、サーバ装置４０、又はサーバ装置５０とがＳＡＣを確立した後、各サーバ装置との間で情報を送受信する際に、公開鍵暗号処理部１０７からセッション鍵を受け取り、受け取ったセッション鍵を暗号鍵又は復号鍵として用い、情報を暗号化してサーバ装置へ送信したり、サーバ装置から受信する暗号化された情報を復号したりする。

【００３４】

（４）メモリカード入出力部１０４

メモリカード入出力部１０４は、メモリカードスロットを含み、メモリカードスロットに、メモリカード２０が挿入されたことを検知すると、その旨を示す信号を制御部１０３へ出力する。また、メモリカード入出力部１０４は、メモリカード２０が挿入されている状態において、制御部１０３とメモリカード２０との間で情報の入出力を行う。

【００３５】

（５）メモリカード認証部１０５

メモリカード認証部１０５は、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成され、前記ＲＯＭ又は前記ＲＡＭには、図３（ａ）に示すパスワードテーブル１２０が格納されている。

パスワードテーブル１２０は１以上のパスワード情報を含み、各パスワード情報は、メモリカード番号と認証用パスワードとを含む。メモリカード番号は、端末１０に挿入して使用可能であるメモリカードを識別するための情報である。認証用パスワードは、対応付けられているメモリカード番号により識別されるメモリカードと端末１０とが共有している情報であり、メモリカードの認証に用いられる２５６ビットデータである。

【００３６】

メモリカード認証部１０５は、制御部１０３から、メモリカード２０がメモリカード入出力部１０４に挿入されたことを示す信号を受け取ると、パスワードテーブル１２０からメモリカード２０に対応したパスワード情報１２１を読み出し、更に、パスワード情報１２１から認証用パスワードＰＷ__０を読み出す。また、メモリカード認証部１０５は、５６ビットの乱数Ｒ__０を生成する。

【００３７】

メモリカード認証部１０５は、生成した乱数Ｒ__０を、制御部１０３及びメモリカード入出力部１０４を介してメモリカード２０へ出力すると共に、乱数Ｒ__０を暗号鍵として用い、認証用パスワードＰＷ__０に暗号アルゴリズムＥを施して暗号文Ｅ１を生成し、生成した暗号文Ｅ１を記憶する。なお、ここで用いられる暗号アルゴリズムＥの一例はＤＥＳ（Data Encryption Standard）である。

【００３８】

メモリカード認証部１０５は、制御部１０３及びメモリカード入出力部１０４を介してメモリカード２０から暗号文Ｅ２を受け取ると、受け取った暗号文Ｅ２と記憶している暗号文Ｅ１とを比較する。Ｅ１とＥ２とが一致する場合、メモリカード認証部１０５は、「認証ＯＫ」を示す信号を制御部１０３へ出力し、Ｅ１とＥ２とが一致しない場合、メモリカード認証部１０５は、「認証ＮＧ」を示す信号を制御部１０３へ出力する。

【００３９】

（６）ＣＲＬ格納部１０６

ＣＲＬ格納部１０６は、ＲＡＭで構成され、内部にＣＲＬを格納している。ＣＲＬは、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器のＩＤが登録され

たリストである。
　ＣＲＬは、ＣＡにより管理されており、端末１０は、ネットワーク６０を介してＣＡからＣＲＬを受信してＣＲＬ格納部１０６に格納する。ここで、端末１０は、ＣＡから常に最新のＣＲＬを受信し、受信した最新のＣＲＬをそれまで格納していたＣＲＬに替えて、ＣＲＬ格納部１０６に格納する。なお、以下では、ＣＲＬ格納部１０６は、最新のＣＲＬとして、図３（ｂ）に示すＣＲＬ１３０を格納しているものとする。
【００４０】
　また、ＣＲＬについては、「American National Standards Institute, American National Standard for financial Services,ANSX9.57:Public Key Cryptography For the Financial Industry: Certificate Management,1997.」に詳しく開示されている。
（７）公開鍵暗号処理部１０７
　公開鍵暗号処理部１０７は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、乱数生成器などから構成される。
【００４１】
　公開鍵暗号処理部１０７は、端末１０がサーバ装置３０、サーバ装置４０及びサーバ装置５０に対してサービス加入要求を行うとき、各サーバ装置との間でＳＡＣを確立する処理を行う。また、公開鍵暗号処理部１０７は、端末１０がサーバ装置３０、サーバ装置４０及びサーバ装置５０に対してサービス利用要求を行うとき、各サーバ装置との間でＳＡＣを確立する処理を行う。なお、ここで用いられる公開鍵暗号は、楕円曲線暗号及びＲＳＡ暗号である。
【００４２】
（楕円曲線上の離散対数問題）
　ここでは、先ず、楕円曲線暗号の安全性の根拠として用いられる楕円曲線上の離散対数問題について簡単に説明する。
　楕円曲線上の離散対数問題とは、Ｅ（ＧＦ（ｐ））を有限体ＧＦ（ｐ）上で定義された楕円曲線とし、楕円曲線Ｅの位数が大きな素数で割り切れる場合に、楕円曲線Ｅに含まれる元Ｇをベースポイントとする。このとき、楕円曲線Ｅに与えられた元Ｙに対して、
　Ｙ＝ｘ＊Ｇ
となる整数ｘが存在するならば、ｘを求めよ、という問題である。
【００４３】
　ここで、ｐは素数、ＧＦ（ｐ）はｐ個の元を持つ有限体である。また、この明細書において、記号「＊」は、楕円曲線に含まれる元を複数回加算する演算を示し、ｘ＊Ｇは、次式に示すように、楕円曲線に含まれる元Ｇをｘ回加算することを意味する。
　ｘ＊Ｇ＝Ｇ＋Ｇ＋Ｇ＋・・・＋Ｇ
　離散対数問題を公開鍵暗号の安全性の根拠とするのは、多くの元を有する有限体ＧＦ（ｐ）に対して、上記問題は極めて難しいからである。
【００４４】
　なお、離散対数問題については、ニイルコブリッツ著　”ア　コウス　イン　ナンバア　セオリイ　アンド　クリプトグラヒイ”(Neal Koblitz , ”A Course in Number theory and Cryptography”, Springer-Verlag,1987)に詳しく述べられている。
（楕円曲線の演算公式についての説明）
　次に、楕円曲線の演算公式について、以下に説明する。
【００４５】
　楕円曲線の方程式を
　$y^2=x^3+ax+b$とし、
任意の点Ｐの座標を（ｘ１，ｙ１）とし、任意の点Ｑの座標を（ｘ２，ｙ２）とする。ここで、Ｒ＝Ｐ＋Ｑで定まる点Ｒの座標を（ｘ３，ｙ３）とする。
　Ｐ≠Ｑの場合、Ｒ＝Ｐ＋Ｑは、加算の演算となる。加算の公式を以下に示す。
【００４６】
　$x3=\{(y2-y1)/(x2-x1)\}^2-x1-x2$

ｙ３＝｛（ｙ２－ｙ１）／（ｘ２－ｘ１）｝（ｘ１－ｘ３）－ｙ１

Ｐ＝Ｑの場合、Ｒ＝Ｐ＋Ｑ＝Ｐ＋Ｐ＝２×Ｐとなり、Ｒ＝Ｐ＋Ｑは、２倍算の演算となる。２倍算の公式を以下に示す。

$x_3 = \{(3x_1^2 + a) / 2y_1^2 - 2x_1$

$y_3 = \{(3x_1^2 + a) / 2y_1\} (x_1 - x_3) - y_1$

なお、上記演算は、楕円曲線が定義される有限体上での演算である。また、楕円曲線の演算公式については、"Efficient elliptic curve exponentiation" (Miyaji, Ono, and Cohen著、Advances in cryptology-proceedings of ICICS'97, Lecture notes in computer science, 1997, Springer-verlag, 282-290.) に詳しく説明されている。

【００４７】

（サービス加入要求）

ここでは、端末１０が、サーバ装置３０に対してサービスへの加入を要求するときの公開鍵暗号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３から乱数Ｒ＿００１０を受け取り、内部に記憶する。乱数Ｒ＿００１０は端末１０自身の秘密鍵であり、ＳＡＣ確立処理に用いられる。なお、乱数Ｒ＿００１０は、メモリカード２０のセキュア領域に格納されており、制御部１０３がメモリカード入出力部１０４を介して読み出したものである。公開鍵暗号処理部１０７は、公開鍵暗号のアルゴリズムとしてＲＳＡ暗号を用い、サーバ装置３０とＳＡＣを確立する。詳細については後述する。公開鍵暗号処理部１０７は、サーバ装置３０との間で確立されたＳＡＣを用い、ネットワーク６０、通信部１０１及び制御部１０３を介して、サーバ装置３０から、楕円曲線のシステムパラメータ「a_1、b_1、p_1、q_1、及び、G_1」を受け取る。

【００４８】

具体例として、$a_1 = -3$

$b_1 = 16461$

$p_1 = 20011$

$q_1 = 20023$

$G_1 = (1, 7553)$

とする。

【００４９】

更に、公開鍵暗号処理部１０７は、サービス用秘密鍵ＳＫを生成する。公開鍵暗号処理部１０７は、生成したサービス用秘密鍵ＳＫとシステムパラメータとを用いて、公開鍵ＰＫ＿Ａ＝ＳＫ＊G_1（ｍｏｄ　p_1）を算出する。公開鍵暗号処理部１０７は、生成したＳＫを、制御部１０３及びメモリカード入出力部１０４を介してメモリカード２０に格納し、算出した公開鍵ＰＫ＿Ａを、サーバ装置３０との間で確立されたＳＡＣを用い、制御部１０３、通信部１０１及びネットワーク６０を介してサーバ装置３０へ送信する。

【００５０】

次に、端末１０が、サーバ装置４０に対してサービスへの加入を要求するときの公開鍵暗号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３から端末１０自身の秘密鍵である乱数Ｒ＿００１０を受け取り、ＲＳＡ暗号を用いて、サーバ装置４０とＳＡＣを確立する。ＳＡＣを確立すると、公開鍵暗号処理部１０７は、制御部１０３からサービス用秘密鍵ＳＫを受け取り、また、サーバ装置４０との間で確立されたＳＡＣを用い、ネットワーク６０、通信部１０１及び制御部１０３を介して、サーバ装置４０から楕円曲線のシステムパラメータ「a_2、b_2、p_2、q_2、及び、G_2」を受け取る。

【００５１】

具体例として、$a_2 = -3$

$b_2 = 16461$

$p_2 = 20011$

$q_2 = 20023$

$G_2 = (18892, 5928)$

とする。公開鍵暗号処理部１０７は、受け取ったＳＫとシステムパラメータとから公開鍵

ＰＫ＿Ｂ＝ＳＫ＊G_2（ｍｏｄ　p_2）を算出し、算出した公開鍵ＰＫ＿Ｂを、サーバ装置４０との間で確立したＳＡＣを用い、制御部１０３、通信部１０１及びネットワーク６０を介してサーバ装置４０へ送信する。

【００５２】

次に、端末１０が、サーバ装置５０に対してサービスへの加入を要求するときの公開鍵暗号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３から端末１０自身の秘密鍵である乱数Ｒ＿００１０を受け取り、ＲＳＡ暗号を用いて、サーバ装置５０とＳＡＣを確立する。ＳＡＣを確立すると、公開鍵暗号処理部１０７は、制御部１０３からＳＫを受け取り、また、サーバ装置５０と確立したＳＡＣを用いて、ネットワーク６０、通信部１０１及び制御部１０３を介して、サーバ装置５０から楕円曲線のシステムパラメータ「a_3、b_3、p_3、q_3、及び、G_3」を受け取る。

【００５３】

具体例として、a_3＝－３
b_3＝１６４６１
p_3＝２００１１
q_3＝２００２３
G_3＝（８８９８，１３２５８）
とする。公開鍵暗号処理部１０７は、ＳＫとシステムパラメータとを用いて、公開鍵ＰＫ＿Ｃ＝ＳＫ＊G_3（ｍｏｄ　p_3）を算出し、算出した公開鍵ＰＫ＿Ｃを、サーバ装置５０との間で確立したＳＡＣを用いて、制御部１０３、通信部１０１及びネットワーク６０を介してサーバ装置５０へ送信する。

【００５４】

上記の様に、端末１０は、サーバ装置３０に対するサービス加入要求時に生成した１個のサービス用秘密鍵ＳＫと、各サーバ装置から受信したシステムパラメータとを用いて、各サーバ装置に対応する３個の公開鍵ＰＫ＿Ａ、ＰＫ＿Ｂ、ＰＫ＿Ｃを生成する。ここで、各サーバ装置から受信したシステムパラメータの内、ベースポイントG_1、G_2、G_3は、それぞれ異なるため、生成される３個の公開鍵は互いに異なる。

【００５５】

（サービス利用要求）

ここでは、端末１０が、サーバ装置３０に対してサービスの利用を要求するときの公開鍵暗号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３からＳＫ、Ｃｅｒｔ＿Ａ及びP_K＿３０を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置３０とＳＡＣを確立する。なお、ＳＫは、端末１０のサービス用秘密鍵であり、メモリカード２０のセキュア領域に格納されている。Ｃｅｒｔ＿Ａは、図１２（ａ）に示す様に、サーバ装置３０から端末１０へ発行された公開鍵証明書であり、端末１０が、サーバ装置３０に対して公開している公開鍵ＰＫ＿Ａ、サーバ装置３０による署名データなどを含む。なお、Ｃｅｒｔ＿Ａは、メモリカード２０の公開鍵格納領域２０４ｃ格納されている。P_K＿３０は、サーバ装置３０の公開鍵であり、記憶部１０８に格納されている。ＳＡＣ確立処理の詳細は後述する。

【００５６】

次に、端末１０が、サーバ装置４０に対してサービスの利用を要求するときの公開鍵暗号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３からＳＫ、Ｃｅｒｔ＿Ｂ及びP_K＿４０を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置４０とＳＡＣを確立する。Ｃｅｒｔ＿Ｂは、図１２（ｂ）に示す様に、サーバ装置４０から端末１０へ発行された公開鍵証明書であり、端末１０がサーバ装置４０に対して公開している公開鍵ＰＫ＿Ｂ、サーバ装置４０による署名データなどを含む。Ｃｅｒｔ＿Ｂは、メモリカード２０の公開鍵格納領域２０４ｃに格納されている。P_K＿４０は、サーバ装置４０の公開鍵であり、記憶部１０８に格納されている。

【００５７】

次に、端末１０が、サーバ装置５０に対してサービスの利用を要求するときの公開鍵暗

号処理部１０７について説明する。公開鍵暗号処理部１０７は、制御部１０３からＳＫ、Ｃｅｒｔ＿Ｃ及びP_K＿５０を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置５０とＳＡＣを確立する。Ｃｅｒｔ＿Ｃは、図１２（ｃ）に示す様に、サーバ装置５０から端末１０へ発行された公開鍵証明書であり、端末１０がサーバ装置５０に対して公開している公開鍵ＰＫ＿Ｃ、サーバ装置５０による署名データなどを含む。Ｃｅｒｔ＿Ｃは、メモリカード２０の公開鍵格納領域２０４ｃに格納されている。P_K＿５０は、サーバ装置５０の公開鍵であり、記憶部１０８に格納されている。

【００５８】

（８）記憶部１０８

記憶部１０８は、制御部１０３から公開鍵P_K＿３０、P_K＿４０及びP_K＿５０を受け取り、受け取った各公開鍵を記憶する。P_K＿３０は、サーバ装置３０の公開鍵であり、P_K＿４０は、サーバ装置４０の公開鍵であり、P_K＿５０は、サーバ装置５０の公開鍵である。

【００５９】

（９）再生部１０９

再生部１０９は、オーディオデコーダ、ビデオデコーダ、バッファ等を備える。図２に示す様に、再生部１０９は外部の出力装置と接続されており、デコードしたコンテンツを出力装置へ出力する。なお、出力装置は、具体的には、モニタ及びスピーカである。

２．メモリカード２０

メモリカード２０は、記録媒体にフラッシュメモリを用いたカード型メモリである。図４は、メモリカード２０の構成を機能的に示す機能ブロック図である。同図に示す様に、メモリカード２０は、入出力部２０１、メモリ制御部２０２、認証部２０３及びメモリ２０４から構成される。

【００６０】

（１）入出力部２０１

入出力部２０１は、複数のピン端子を含み、メモリカード２０が端末１０のメモリカード入出力部１０４に挿入された状態において、前記複数のピン端子により、端末１０のメモリカード入出力部１０４から受信したデータをメモリ制御部２０２へ出力し、メモリ制御部２０２から受け取ったデータをメモリカード入出力部１０４へ出力する。

【００６１】

一例として、入出力部２０１は、メモリカード２０が端末１０に挿入されると、メモリ制御部２０２を介して認証部２０３が記憶しているメモリカード番号「２０」を受け取り、受け取ったメモリカード番号「２０」をメモリカード入出力部１０４へ出力する。その他、入出力部２０１が送受信するデータは、後述する情報セキュリティシステム１の動作の説明において順次説明する。

【００６２】

（２）メモリ制御部２０２

メモリ制御部２０２は、入出力部２０１を介して端末１０から受け取る指示に従い、メモリ２０４からデータを読み出し、読み出したデータを入出力部２０１を介して端末１０へ送信する。また、メモリ制御部２０２は、入出力部２０１を介して端末１０からデータを受信し、受信したデータをメモリ２０４に格納する。

【００６３】

メモリ制御部２０２は、入出力部２０１を介して端末１０から乱数Ｒ＿０を受信し、受信した乱数Ｒ＿０を認証部２０３へ出力する。また、メモリ制御部２０２は、認証部２０３から暗号文Ｅ２を受け取り、受け取ったＥ２を入出力部２０１を介して端末１０へ出力する。

（３）認証部２０３

認証部２０３は、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを備える。ＲＯＭ又はＲＡＭには、認証用プログラムが記憶されており、マイクロプロセッサにより前記認証用プログラムが実行される。なお、ＲＯＭには予めメモリカード番号「２０」と認証用パスワー

ド「ＰＷ＿０」とが記憶されている。メモリカード番号「２０」は、メモリカード２０を識別するための番号である。ＰＷ＿０は、端末１０と共有している秘密のデータであって、端末１０のメモリカード認証部１０５との間で行われるチャレンジ-レスポンス型の認証処理に用いられる。

【００６４】

認証部２０３は、入出力部２０１を介して、端末１０から乱数Ｒ＿０を受信し、受信した乱数Ｒ＿０を暗号鍵として用い、認証用パスワードＰＷ＿０に暗号アルゴリズムＥを施して暗号文Ｅ２を生成する。認証部２０３は、生成した暗号文Ｅ２を、メモリ制御部２０２及び入出力部２０１を介して端末１０へ送信する。

なお、ここで用いられる暗号アルゴリズムＥの一例は、ＤＥＳである。

【００６５】

（４）メモリ２０４

メモリ２０４は、具体的にはＥＥＰＲＯＭなどから構成される記憶装置であって、セキュア領域２０４ａと、コンテンツ格納領域２０４ｂと、公開鍵格納領域２０４ｃとを備える。

セキュア領域２０４ａは、内部解析、改竄が物理的及び理論的に不可能な耐タンパー性を有する記憶領域である。セキュア領域２０４ａは、端末１０の秘密鍵であるＲ＿００１０と、サービス用秘密鍵ＳＫとを内部に格納する。なお、メモリ２０４全体の記憶容量に対して、セキュア領域２０４ａの記憶容量は微小なサイズである。

【００６６】

コンテンツ格納領域２０４ｂは、端末１０が、サーバ装置３０、サーバ装置４０及びサーバ装置５０から取得したコンテンツを格納する。

公開鍵格納領域２０４ｃは、ＣＡから取得する公開鍵証明書Ｃｅｒｔ＿００１０、及び、サーバ装置３０から取得する公開鍵証明書Ｃｅｒｔ＿Ａと、サーバ装置４０から取得する公開鍵証明書Ｃｅｒｔ＿Ｂと、サーバ装置５０から取得する公開鍵証明書Ｃｅｒｔ＿Ｃとを内部に格納する。

【００６７】

３．サーバ装置３０

サーバ装置３０は、コンテンツ配信業者が有する装置であり、ネットワーク６０を介して接続された端末１０からサービス加入要求を受け付けると、端末１０を登録する。また、サーバ装置３０は、登録済みである端末１０からサービス利用要求を受け付けると、端末１０にコンテンツを提供する。

【００６８】

図５は、サーバ装置３０の構成を機能的に示す機能ブロック図である。同図に示す様に、サーバ装置３０は、通信部３０１、制御部３０２、ＣＲＬ格納部３０３、Ｃｅｒｔ管理部３０４、登録情報管理部３０５、公開鍵暗号処理部３０６及びコンテンツ格納部３０７から構成される。

サーバ装置３０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット等から構成されるコンピュータシステムである。

【００６９】

（１）通信部３０１

通信部３０１は、Ｗｅｂブラウザを備えるネットワーク接続ユニットであって、ネットワーク６０を介して端末１０と接続されている。

通信部３０１は、端末１０から情報を受信し、受信した情報を制御部３０２へ出力する。また、通信部３０１は、制御部３０２から情報を受け取り、受け取った情報を端末１０へ送信する。

【００７０】

通信部３０１が端末１０から受信する情報の具体例は、公開鍵ＰＫ＿Ａ、ＳＡＣ確立に用いる署名データ及び鍵情報などである。通信部３０１が端末１０へ送信する情報の具体例は、公開鍵証明書Ｃｅｒｔ＿Ａ、ＳＡＣ確立に用いる署名データ、鍵情報、楕円曲線の

システムパラメータ、コンテンツなどである。
　更に、通信部３０１は、ネットワーク６０を介して、ＣＡと接続されており、通信部３０１は、ＣＡとの間で以下の様に情報の送受信を行う。
【００７１】
　通信部３０１は、ネットワーク６０を介してＣＡから常に最新のＣＲＬを受信し、受信した最新のＣＲＬを、制御部３０２を介してＣＲＬ格納部３０３に格納する。
　通信部３０１は、制御部３０２を介して公開鍵暗号処理部３０６から公開鍵「ＰＫ＿００３０」を受け取り、受け取った公開鍵をネットワーク６０を介してＣＡへ送信する。また、通信部３０１は、ネットワーク６０を介してＣＡから公開鍵「ＰＫ＿００３０」に対応する公開鍵証明書「Ｃｅｒｔ＿００３０」を受信し、受信した公開鍵証明書を制御部３０２へ出力する。
【００７２】
　通信部３０１は、ネットワーク６０を介してＣＡから楕円曲線のシステムパラメータを取得し、取得したシステムパラメータを制御部３０２へ出力する。
　（２）制御部３０２
　制御部３０２は、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成され、コンピュータプログラムをマイクロプロセッサが実行することにより、制御部３０２は、サーバ装置３０の全体を制御する。
【００７３】
　（ａ）制御部３０２は、端末１０との通信に先立ち、ＣＡから公開鍵証明書の発行を受ける。より具体的には、通信部３０１は、公開鍵暗号処理部３０６から出力される公開鍵「ＰＫ＿００３０」と予め内部に記憶している自身のデバイスＩＤ「ＩＤ＿００３０」とを、通信部３０１を介してＣＡへ送信する。制御部３０２は、通信部３０１を介して公開鍵「ＰＫ＿００３０」に対応する公開鍵証明書「Ｃｅｒｔ＿００３０」をＣＡから受信し、受信した公開鍵証明書を、Ｃｅｒｔ管理部３０４に出力する。
【００７４】
　（ｂ）制御部３０２は、端末１０からサービス加入要求を受け付けると、Ｃｅｒｔ管理部３０４から「Ｃｅｒｔ＿００３０」を読み出す。更に、制御部３０２は、端末１０とＳＡＣを確立する指示を公開鍵暗号処理部３０６に出力する。端末１０との間でＳＡＣが確立されると、制御部３０２は、ＣＡから取得した楕円曲線のシステムパラメータ「a_1、b_1、p_1、q_1、及び、G_1」を、公開鍵暗号処理部３０６から受け取るセッション鍵で暗号化したのち、通信部３０１及びネットワーク６０を介して端末１０へ送信する。
【００７５】
　具体的に、サーバ装置３０が受信するシステムパラメータは、
　a_1＝－３
　b_1＝１６４６１
　p_1＝２００１１
　q_1＝２００２３
　G_1＝（１，７５５３）
であるとする。
【００７６】
　（ｃ）ＳＡＣ確立処理の一環として、ＣＲＬ格納部３０３から最新のＣＲＬを読み、認証相手である端末１０が、無効化された装置であるか否かを判断する。
　（ｄ）制御部３０２は、端末１０からＣｅｒｔ＿Ａを含むサービス利用要求を受け取ると、Ｃｅｒｔ＿Ａが確かにサーバ装置３０自身が端末１０へ発行した公開鍵証明書であるか否か判定する。このとき、制御部３０２は、登録情報管理部３０５に管理されている登録情報を参照する。端末１０から受信したＣｅｒｔ＿Ａが正しければ、制御部３０２は、公開鍵暗号処理部３０６へ、ＳＡＣ確立処理の指示を出す。
【００７７】
　（ｅ）制御部３０２は、サーバ装置３０と端末１０とがＳＡＣを確立した後、端末１０

との間で情報を送受信する際に、公開鍵暗号処理部３０６からセッション鍵を受け取り、受け取ったセッション鍵を暗号鍵又は復号鍵として用い、情報を暗号化して端末１０へ送信したり、端末１０から受信する暗号化された情報を復号したりする。具体例として、制御部３０２は、サービス提供時の処理として、端末１０とＳＡＣを確立した後、公開鍵暗号処理部３０６からセッション鍵を受け取り、コンテンツ格納部３０７からコンテンツを読み出す。制御部３０２は、読み出したコンテンツをセッション鍵で暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを、通信部３０１を介して端末１０へ送信する。

【００７８】

（３）ＣＲＬ格納部３０３

ＣＲＬ格納部３０３は、ＲＡＭで構成され、内部にＣＲＬを格納している。ＣＲＬは、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器のＩＤが登録されたリストである。ＣＲＬは、ネットワーク６０を介してＣＡからサーバ装置３０へ送信される。ここで、サーバ装置３０は、ＣＡから常に最新のＣＲＬを受信し、受信した最新のＣＲＬをそれまで格納していたＣＲＬに替えて、ＣＲＬ格納部３０３に格納する。なお、以下では、ＣＲＬ格納部３０３は、端末１０のＣＲＬ格納部１０６と同様に最新のＣＲＬとして、図３（ｂ）に示すＣＲＬ１３０を格納しているものとする。

【００７９】

（４）Ｃｅｒｔ管理部３０４

Ｃｅｒｔ管理部３０４は、通信部３０１及び制御部３０２を介してＣＡから公開鍵証明書Ｃｅｒｔ＿００３０を受け取り、受け取ったＣｅｒｔ＿００３０を内部に格納する。

（５）登録情報管理部３０５

登録情報管理部３０５は、公開鍵暗号処理部３０６により公開鍵証明書が発行された端末の登録情報を管理する。登録情報は、登録された端末の公開鍵や端末に割り振った会員番号、ユーザに関する情報などを含み、登録され端末及びユーザの管理に用いられる。また、登録情報は、制御部３０２が端末１０から送信されたＣｅｒｔを検証するときに用いられる。

【００８０】

（６）公開鍵暗号処理部３０６

公開鍵暗号処理部３０６は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、乱数生成器等から構成される。

公開鍵暗号処理部３０６は、端末１０との通信に先立ち、乱数生成器で乱数Ｒ＿００３０を生成し、生成したＲ＿００３０に基づき、公開鍵ＰＫ＿００３０を生成する。公開鍵暗号処理部３０６は、生成した公開鍵ＰＫ＿００３０を制御部３０２、通信部３０１を介してＣＡへ送信する。

【００８１】

（端末１０の登録）

公開鍵暗号処理部３０６は、秘密鍵K_S＿３０を生成し、制御部３０２から楕円曲線のシステムパラメータを受け取る。公開鍵暗号処理部３０６は、秘密鍵K_S＿３０とシステムパラメータとから、K_P＿３０＝K_S＿３０＊G_1（ｍｏｄ　p_1）を計算し、公開鍵K_P＿３０を生成する。公開鍵暗号処理部３０６は、生成した公開鍵K_P＿３０を、制御部３０２へ出力する。

【００８２】

公開鍵暗号処理部３０６は、サービス加入、登録処理において、端末１０から公開鍵ＰＫ＿Ａを受け取ると、受け取った公開鍵ＰＫ＿Ａに基づき、公開鍵証明書Ｃｅｒｔ＿Ａを生成し、生成したＣｅｒｔ＿Ａを制御部３０２へ出力する。

（端末１０へサービス提供）

公開鍵暗号処理部３０６は、制御部３０２からＳＡＣ確立処理の指示を受けると、端末１０とＳＡＣを確立しセッション鍵を生成する。ＳＡＣ確立の詳細については後述する。

【００８３】

（７）コンテンツ格納部３０７
コンテンツ格納部３０７は、具体的にはハードディスクドライブユニットであって、内部にコンテンツを格納している。
４．サーバ装置４０
サーバ装置４０は、サーバ装置３０を有するコンテンツ配信業者とは異なるコンテンツ配信業者が有する装置である。サーバ装置４０は、ネットワーク６０を介して接続された端末１０からサービス加入要求を受け付けると、端末１０を登録する。また、サーバ装置４０は、内部にコンテンツを格納しており、登録済みである端末１０からサービス利用要求を受け付けると、端末１０にコンテンツを提供する。
【００８４】
サーバ装置４０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット等から構成されるコンピュータシステムである。サーバ装置４０は、図５に示したサーバ装置３０と同様の構成を有するため、サーバ装置４０の構成は図示していない。以下では、サーバ装置３０と異なる部分を中心に、サーバ装置４０について説明する。
（ａ）サーバ装置４０は、端末１０との通信に先立ち、公開鍵ＰＫ＿００４０を生成し、ＰＫ＿００４０をＣＡに送信し、ＣＡから公開鍵証明書Ｃｅｒｔ＿００４０の発行を受ける。図９（ｃ）に示す公開鍵証明書１６０は、Ｃｅｒｔ＿００４０のデータ構成を示す図である。ＣＡから取得したＣｅｒｔ＿００４０は、端末１０とＳＡＣを確立する処理に用いられる。
【００８５】
（ｂ）サーバ装置４０は、ＣＡから楕円曲線のシステムパラメータを受信する。ここで、サーバ装置４０が受信するシステムパラメータの組は、サーバ装置４０にユニークであるとする。
具体的に、サーバ装置４０が受信するシステムパラメータは、
$a_2 = -3$
$b_2 = 16461$
$p_2 = 20011$
$q_2 = 20023$
$G_2 = (18892, 5928)$
であるとする。
【００８６】
サーバ装置４０は、秘密鍵K_S＿４０を生成し、生成したK_S＿４０とＣＡから受信したシステムパラメータとから、楕円曲線上の計算により、K_P＿４０＝K_S＿４０＊G_2（ｍｏｄ　p_2）を算出し、公開鍵K_P＿４０を生成する。
サーバ装置４０は、端末１０とＳＡＣを確立した後、ＣＡから受信したシステムパラメータと、生成した公開鍵K_P＿４０とを、端末１０へ送信する。
【００８７】
（ｃ）サーバ装置４０は、端末１０から公開鍵ＰＫ＿Ｂを受信し、受信した公開鍵ＰＫ＿Ｂに対して、公開鍵証明書Ｃｅｒｔ＿Ｂを発行する。図１２（ｂ）に示した公開鍵証明書２２０は、Ｃｅｒｔ＿Ｂのデータ構成を示す図である。
（ｄ）サーバ装置４０は、端末１０から公開鍵証明書Ｃｅｒｔ＿Ｂを含むサービス利用要求を受信すると、Ｃｅｒｔ＿Ｂを検証する。Ｃｅｒｔ＿Ｂの検証に成功すると、サーバ装置４０は、端末１０とＳＡＣを確立し、端末１０へコンテンツを送信する。
【００８８】
５．サーバ装置５０
サーバ装置５０は、サーバ装置３０を有するコンテンツ配信業者、及び、サーバ装置４０を有するコンテンツ配信業者とは異なるコンテンツ配信業者が有する装置である。サーバ装置５０は、ネットワーク６０を介して接続された端末１０からサービス加入要求を受け付けると、端末１０を登録する。また、サーバ装置５０は、内部にコンテンツを格納しており、登録済みである端末１０からサービス利用要求を受け付けると、端末１０にコン

テンツを提供する。

【００８９】

サーバ装置５０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット等から構成されるコンピュータシステムである。サーバ装置５０は、図５に示したサーバ装置３０と同様の構成を有するため、サーバ装置５０の構成は図示していない。以下では、サーバ装置３０及びサーバ装置４０と異なる部分を中心に、サーバ装置５０について説明する。

【００９０】

（ａ）サーバ装置５０は、端末１０との通信に先立ち、公開鍵ＰＫ＿００５０を生成し、ＰＫ＿００５０をＣＡに送信し、ＣＡから公開鍵証明書Ｃｅｒｔ＿００５０の発行を受ける。図９（ｄ）に示す公開鍵証明書１７０は、Ｃｅｒｔ＿００５０のデータ構成を示す図である。ＣＡから取得したＣｅｒｔ＿００５０は、端末１０とＳＡＣを確立する処理に用いられる。

【００９１】

（ｂ）サーバ装置５０は、ＣＡから楕円曲線のシステムパラメータを受信する。ここで、サーバ装置５０が受信するシステムパラメータの組は、サーバ装置５０にユニークであるとする。

具体的に、サーバ装置５０が受信するシステムパラメータは、

a_3＝－３

b_3＝１６４６１

p_3＝２００１１

q_3＝２００２３

G_3＝（８８９８、１３２５８）

であるとする。

【００９２】

サーバ装置５０は、秘密鍵K_S＿５０を生成し、生成したK_S＿５０とＣＡから受信したシステムパラメータとから、楕円曲線上の計算により、K_P＿５０＝K_S＿５０＊G_3（ｍｏｄ　p_3）を算出し、公開鍵K_P＿５０を生成する。

サーバ装置５０は、端末１０とＳＡＣを確立した後、ＣＡから受信したシステムパラメータと、生成した公開鍵K_P＿５０とを、端末１０へ送信する。

【００９３】

（ｃ）サーバ装置５０は、端末１０から公開鍵ＰＫ＿Ｃを受信し、受信した公開鍵ＰＫ＿Ｃに対して、公開鍵証明書Ｃｅｒｔ＿Ｃを発行する。図１２（ｃ）に示した公開鍵証明書２３０は、Ｃｅｒｔ＿Ｃのデータ構成を示す図である。

（ｄ）サーバ装置５０は、端末１０から公開鍵証明書Ｃｅｒｔ＿Ｃを含むサービス利用要求を受信すると、Ｃｅｒｔ＿Ｃを検証する。Ｃｅｒｔ＿Ｃの検証に成功すると、サーバ装置５０は、端末１０とＳＡＣを確立し、端末１０へコンテンツを送信する。

【００９４】

＜動作＞

ここでは、フローチャートを用いて、情報セキュリティシステム１の動作について説明する。

（１）全体の動作１（サービス加入、登録時）

図６及び図１５は、情報セキュリティシステム１全体の動作を示すフローチャートである。図６は「サービス加入、登録時」における情報セキュリティシステム１の動作を示し、図１５は「サービス利用時」における情報セキュリティシステム１の動作を示す。

【００９５】

先ず、メモリカード２０が端末１０のメモリカード入出力部１０４に挿入されると（ステップＳ１０１）、端末１０は、メモリカード２０を認証する（ステップＳ１０２）。端末１０は、メモリカード２０の認証に失敗すると（ステップＳ１０３でＮＧ）、処理を終了する。端末１０は、メモリカード２０の認証に成功すると（ステップＳ１０３でＯＫ）

、ＣＡから公開鍵証明書の発行を受ける（ステップＳ１０４）。

【００９６】

サーバ装置３０は、予め、ＣＡから公開鍵証明書の発行を受ける（ステップＳ１０５）。同様に、サーバ装置４０は、予め、ＣＡから公開鍵証明書の発行を受ける（ステップＳ１０６）。同様に、サーバ装置５０は、予め、ＣＡから公開鍵証明書の発行を受ける（ステップＳ１０７）。

続いて、端末１０及びサーバ装置３０は、サービス加入、登録処理を行う（ステップＳ１０８）。次に、端末１０とサーバ装置４０は、サービス加入、登録処理を行う（ステップＳ１０９）。次に、端末１０とサーバ装置５０は、サービス加入、登録処理を行う（ステップＳ１１０）。

【００９７】

以上が「サービス加入、登録時」における処理である。

以下、図１５に続くが、ここでは、説明の便宜上、図７以降のフローチャートを用いて、サービス加入、登録時における処理の詳細について先に説明し、その後、図１５について説明する。

（２）メモリカード２０の認証処理

ここでは、図７に示すフローチャートを用いてメモリカード２０の認証処理について説明する。なお、ここで説明する動作は、図６のステップＳ１０２の詳細である。

【００９８】

端末１０のメモリカード入出力部１０４に、メモリカード２０が挿入されている状態において、端末１０のメモリカード認証部１０５は、乱数Ｒ＿０を生成し（ステップＳ２０１）、生成した乱数Ｒ＿０を内部に保持すると共に、メモリカード入出力部１０４を介してメモリカード２０へ送信し、メモリカード２０は乱数Ｒ＿０を受信する（ステップＳ２０２）。

【００９９】

メモリカード２０の認証部２０３は、入出力部２０１及びメモリ制御部２０２を介して乱数Ｒ＿０を受け取ると、Ｒ＿０を暗号鍵として用い、内部に保持している認証用パスワードＰＷ＿０に暗号アルゴリズムＥを施して暗号文Ｅ２を生成する（ステップＳ２０３）。一方、メモリカード認証部１０５は、ステップＳ２０１で生成した乱数Ｒ＿０を暗号鍵として用い、メモリカード２０と共有している認証用パスワードＰＷ＿０に暗号アルゴリズムＥを施して暗号文Ｅ１を生成する（ステップＳ２０４）。

【０１００】

メモリカード２０の認証部２０３は、ステップＳ２０３で生成した暗号文Ｅ２を端末１０へ送信し、端末１０は、暗号文Ｅ２を受信する（ステップＳ２０５）。端末１０のメモリカード認証部１０５は、メモリカード入出力部１０４及び制御部１０３を介して暗号文Ｅ２を受け取ると、受け取った暗号文Ｅ２と、ステップＳ２０４で生成した暗号文Ｅ１とを比較する（ステップＳ２０６）。

【０１０１】

暗号文Ｅ１と暗号文Ｅ２とが一致する場合（ステップＳ２０７でＹＥＳ）、端末１０はメモリカード２０の認証に成功であり、メモリカード認証部１０５は、制御部１０３へ「認証ＯＫ」を示す信号を出力する（ステップＳ２０８）。次に、端末１０は、図６のステップＳ１０３に戻り処理を続ける。

暗号文Ｅ１と暗号文Ｅ２とが一致しない場合（ステップＳ２０７でＮＯ）、端末１０は、メモリカード２０の認証に失敗であり、メモリカード認証部１０５は、制御部１０３へ「認証ＮＧ」を示す信号を出力する（ステップＳ２０９）。次に、端末１０は、図６のステップＳ１０３に戻り処理を続ける。

【０１０２】

（３）ＣＡから公開鍵証明書（Ｃｅｒｔ）の発行を受ける処理

ここでは、図８に示すフローチャートを用いて、端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０が、ＣＡから公開鍵証明書の発行を受ける処理について説明す

る。なお、ここで説明する動作は、図６のステップＳ１０４、ステップＳ１０５、ステップＳ１０６及びステップＳ１０７の詳細である。

【０１０３】

端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０の公開鍵暗号処理部は、それぞれ乱数生成器により乱数Ｒ＿Ｌを生成し（ステップＳ３０１）、更に、生成した乱数Ｒ＿Ｌから公開鍵ＰＫ＿Ｌを生成する（ステップＳ３０２）。ここで、端末１０は、Ｌ＝００１０、サーバ装置３０は、Ｌ＝００３０、サーバ装置４０は、Ｌ＝００４０、サーバ装置５０は、Ｌ＝００５０である。なお、乱数Ｒ＿Ｌから公開鍵ＰＫ＿Ｌを生成するアルゴリズムは限定しない。一例としては、ＲＳＡ暗号である。

【０１０４】

端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０の公開鍵暗号処理部は、生成した公開鍵ＰＫ＿Ｌを制御部へ出力する。制御部は、公開鍵ＰＫ＿Ｌと、内部に記憶している自身のデバイスＩＤとを含む情報を、通信部を介してＣＡに送信し、ＣＡは、公開鍵ＰＫ＿Ｌとデバイスを含む情報を受信する（ステップＳ３０３）。

ＣＡは、ステップＳ３０３で受信した情報の送信元（公開鍵証明書の依頼元）について、公開鍵、メールアドレス、ユーザ、ユーザが属する組織などが確かに存在し、且つ、正しいことを検証する（ステップＳ３０４）。

【０１０５】

依頼元が不正な場合（ステップＳ３０５でＮＯ）、ＣＡは、処理を終了する。

依頼元が正当な場合（ステップＳ３０５でＹＥＳ）、ＣＡは、受信した公開鍵ＰＫ＿Ｌ及びデバイスＩＤに署名データＳｉｇ＿ＬＣＡを付加し、公開鍵証明書Ｃｅｒｔ＿Ｌを生成する（ステップＳ３０６）。ＣＡは、生成した公開鍵証明書Ｃｅｒｔ＿Ｌを依頼元の端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０へ送信し、端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０は、公開鍵証明書Ｃｅｒｔ＿Ｌを受信する（ステップＳ３０７）。

【０１０６】

端末１０は、受信した公開鍵証明書Ｃｅｒｔ＿００１０を、制御部１０３及びメモリカード入出力部１０４を介して、メモリカード２０の公開鍵格納領域２０４ｃに格納する（ステップＳ３０８）。ここで、端末１０がＣＡから受信した公開鍵証明書Ｃｅｒｔ＿００１０のデータ構成を図９（ａ）に示す。同図に示す様に、Ｃｅｒｔ＿００１０は、ＩＤ＿００１０と、ＰＫ＿００１０と、Ｓｉｇ＿００１０ＣＡとを含む。なお、ＩＤ＿００１０は、端末１０のデバイスＩＤである。

【０１０７】

サーバ装置３０は、ステップＳ３０７で受信した公開鍵証明書Ｃｅｒｔ＿００３０を、制御部３０２を介してＣｅｒｔ管理部３０４に格納する（ステップＳ３０８）。図９（ｂ）は、サーバ装置３０がＣＡから受信した公開鍵証明書Ｃｅｒｔ＿００３０のデータ構成を示す図である。同図に示す様に、Ｃｅｒｔ＿００３０は、ＩＤ＿００３０と、ＰＫ＿００３０と、ＩＤ＿００３０と、Ｓｉｇ＿００３０ＣＡとを含む。なお、ＩＤ＿００３０は、サーバ装置３０のデバイスＩＤである。

【０１０８】

サーバ装置４０及びサーバ装置５０も同様に、それぞれがステップＳ３０７で受信した公開鍵証明書Ｃｅｒｔ＿００４０及びＣｅｒｔ＿００５０を内部に格納する（ステップＳ３０８）。図９（ｃ）は、サーバ装置４０がＣＡから受信した公開鍵証明書Ｃｅｒｔ＿００４０のデータ構成を示す図であり、図９（ｄ）は、サーバ装置５０がＣＡから受信した公開鍵証明書Ｃｅｒｔ＿００５０のデータ構成を示す図である。

【０１０９】

ＣＡから公開鍵証明書を取得すると、端末１０及びサーバ装置３０は、図６のステップＳ１０８の処理に続く。サーバ装置４０は、ステップＳ１０９の処理に続き、サーバ装置５０は、ステップＳ１１０の処理に続く。

（４）サービス加入、登録処理

ここでは、図１０及び図１１に示すフローチャートを用いて、端末１０とサーバ装置３０とによるサービス加入、登録処理（図６のステップＳ１０８）、端末１０とサーバ装置４０とによるサービス加入、登録処理（図６のステップＳ１０９）、及び、端末１０とサーバ装置５０とによるサービス加入、登録処理（図６のステップＳ１１０）の動作について説明する。なお、ここでは、サーバ装置３０、サーバ装置４０及びサーバ装置５０を、単に「サーバ装置」と呼称することがある。

【０１１０】

端末１０において、操作入力部１０２を介してユーザの入力を受け付けることにより、サーバ装置に対するサービス加入要求が発生すると（ステップＳ４０１）、端末１０とサーバ装置との間でＳＡＣ確立の処理を行う（ステップＳ４０２）。

サーバ装置は、ＣＡから楕円曲線$y^2 = x^3 + ax + b$のシステムパラメータを取得する（ステップＳ４０３）。ここで、サーバ装置３０がＣＡから取得するシステムパラメータは「a_1、b_1、p_1、q_1、及び、G_1」であり、サーバ装置４０がＣＡから取得するシステムパラメータは「a_2、b_2、p_2、q_2、及び、G_2」であり、サーバ装置５０がＣＡから取得するシステムパラメータは「a_3、b_3、p_3、q_3、及び、G_3」である。

【０１１１】

サーバ装置の制御部は、取得したシステムパラメータを、ステップＳ４０２のＳＡＣ確立処理で端末１０と共有したセッション鍵を暗号鍵として用い、暗号化する（ステップＳ４０４）。なお、ここで用いる暗号アルゴリズムの一例はＤＥＳ（Data Encryption Standard）である。サーバ装置の制御部は、暗号化したシステムパラメータを、通信部及びネットワーク６０を介して端末１０へ送信し、端末１０の通信部１０１は、システムパラメータを受信する（ステップＳ４０５）。

【０１１２】

端末１０の制御部１０３は、ステップＳ４０２のＳＡＣ確立処理でサーバ装置と共有したセッション鍵を復号鍵として用い、暗号化されたシステムパラメータを復号する（ステップＳ４０６）。端末１０の公開鍵暗号処理部１０７は、サービス用秘密鍵ＳＫを既に生成しており、メモリカード２０のセキュア領域２０４ａにＳＫが格納されている場合（ステップＳ４０７でＹＥＳ）、ステップＳ４０９に進む。端末１０の公開鍵暗号処理部１０７は、サービス用秘密鍵ＳＫを未だ生成しておらず、メモリカード２０のセキュア領域２０４ａにＳＫが格納されていない場合（ステップＳ４０７でＮＯ）、乱数生成器により、サービス用秘密鍵ＳＫを生成する（ステップＳ４０８）。

【０１１３】

公開鍵暗号処理部１０７は、サービス用秘密鍵ＳＫとサーバ装置から取得したシステムパラメータとを用いて、次式を計算することにより、公開鍵ＰＫ＿Ｎを生成する（ステップＳ４０９）。

$PK\_N = SK * G \pmod{p}$、Ｎ＝Ａ、Ｂ、及び、Ｃ

なお、サービス用秘密鍵ＳＫは、ステップＳ４０８において生成した鍵データ、若しくは、既に生成されてメモリカード２０のセキュア領域２０４ａに格納されている鍵データである。

【０１１４】

ＰＫ＿Ａは、サーバ装置３０から受信するシステムパラメータに基づき生成された公開鍵であり、ＰＫ＿Ｂは、サーバ装置４０から受信するシステムパラメータに基づき生成された公開鍵であり、ＰＫ＿Ｃは、サーバ装置５０から受信するシステムパラメータに基づき生成された公開鍵である。

次に、端末１０の制御部１０３は、セッション鍵を暗号鍵として用い、生成した公開鍵ＰＫ＿Ｎを暗号化し（ステップＳ４１０）、暗号化したＰＫ＿Ｎを、通信部１０１及びネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部は、暗号化された公開鍵ＰＫ＿Ｎを受信する（ステップＳ４１１）。サーバ装置の制御部は、暗号化された公開鍵ＰＫ＿Ｎをセッション鍵を用いて復号する（ステップＳ４１２）。

【０１１５】

続いて、サーバ装置の公開鍵暗号処理部は、端末１０から受信した公開鍵ＰＫ＿Ｎに対して公開鍵証明書Ｃｅｒｔ＿Ｎを生成する（ステップＳ４１３）、次に、公開鍵暗号処理部は、乱数生成器を用いて秘密鍵Ｋｓ＿Ｍを生成し（Ｍ＝３０、４０、及び、５０）、生成した秘密鍵Ｋｓ＿Ｍから公開鍵Ｋｐ＿Ｍ＝Ｋｓ＿Ｍ＊Ｇを算出する（ステップＳ４１５）。Ｇは、楕円曲線のベースポイントである。サーバ装置の制御部は、セッション鍵を暗号鍵として用い、公開鍵証明書Ｃｅｒｔ＿Ｎ及び公開鍵Ｋｐ＿Ｍを暗号化し、暗号化したＣｅｒｔ＿Ｎ及びＫｐ＿Ｍを通信部及びネットワーク６０を介して端末１０へ送信し、端末１０の通信部１０１は、暗号化されたＣｅｒｔ＿Ｎ及びＫｐ＿Ｍを受信する（ステップＳ４１７）。

【０１１６】

端末１０の制御部１０３は、受信したＣｅｒｔ＿Ｎ及びＫｐ＿Ｍをセッション鍵を用いて復号し（ステップＳ４１８）、復号した公開鍵証明書Ｃｅｒｔ＿Ｎをメモリカード入出力部１０４を介して、メモリカード２０のセキュア領域２０４ａに格納し（ステップＳ４１９）、サーバ装置の公開鍵Ｋｐ＿Ｍを記憶部１０８に格納
する（ステップＳ４２０）。

【０１１７】

一方、サーバ装置の登録情報管理部は、端末１０に関する登録情報を生成して管理する（ステップＳ４２１）。登録情報は、端末１０の公開鍵や端末１０に割り振った会員番号などを含む。

ここで、各サーバ装置が生成し、端末１０へ発行する公開鍵証明書Ｃｅｒｔ＿Ｎについて図１２を用いて説明する。

【０１１８】

図１２（ａ）は、サーバ装置３０が端末１０に発行するＣｅｒｔ＿Ａのデータ構成を示す図である。同図に示す様に、Ｃｅｒｔ＿Ａは、サービスＩＤ「ＳＩＤ＿０１２３Ａ」、会員番号「ＮＯ＿０００１」、公開鍵「ＰＫ＿Ａ」及び署名データ「Ｓｉｇ＿Ａ」から構成される。

サービスＩＤ「ＳＩＤ＿０１２３Ａ」は、サーバ装置３０が提供するサービスの内、端末１０が利用するサービスの種類を示す。会員番号「ＮＯ＿０００１」は、サーバ装置３０に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「ＰＫ＿Ａ」は、端末１０が、サービス用秘密鍵ＳＫと、サーバ装置３０から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「Ｓｉｇ＿Ａ」は、サーバ装置３０が、「ＳＩＤ＿０１２３Ａ」、「ＮＯ＿０００１」及び「ＰＫ＿Ａ」に対し、署名アルゴリズムを施して生成したデータである。

【０１１９】

図１２（ｂ）は、サーバ装置４０が端末１０に発行するＣｅｒｔ＿Ｂのデータ構成を示す図である。同図に示す様に、Ｃｅｒｔ＿Ｂは、サービスＩＤ「ＳＩＤ＿０３２１Ｂ」、会員番号「ＮＯ＿００２５」、公開鍵「ＰＫ＿Ｂ」及び署名データ「Ｓｉｇ＿Ｂ」から構成される。

サービスＩＤ「ＳＩＤ＿０３２１Ｂ」は、サーバ装置４０が提供するサービスの内、端末１０が利用するサービスの種類を示す。会員番号「ＮＯ＿００２５」は、サーバ装置４０に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「ＰＫ＿Ｂ」は、端末１０が、サービス用秘密鍵ＳＫと、サーバ装置４０から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「Ｓｉｇ＿Ｂ」は、サーバ装置４０が、「ＳＩＤ＿０３３２１Ｂ」、「ＮＯ＿００２５」及び「ＰＫ＿Ｂ」に対し、署名アルゴリズムを施して生成したデータである。

【０１２０】

図１２（ｃ）は、サーバ装置５０が端末１０に発行するＣｅｒｔ＿Ｃのデータ構成を示す図である。同図に示す様に、Ｃｅｒｔ＿Ｃは、サービスＩＤ「ＳＩＤ＿０１３２Ｃ」、会員番号「ＮＯ＿３２１５」、公開鍵「ＰＫ＿Ｃ」及び署名データ「Ｓｉｇ＿Ｃ」から構成される。

サービスＩＤ「ＳＩＤ＿０１３２Ｃ」は、サーバ装置５０が提供するサービスの内、端末１０が利用するサービスの種類を示す。会員番号「ＮＯ＿３２１５」は、サーバ装置５０に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「ＰＫ＿Ｃ」は、端末１０が、サービス用秘密鍵ＳＫと、サーバ装置５０から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「Ｓｉｇ＿Ｃ」は、サーバ装置５０が、「ＳＩＤ＿０１３２Ｃ」、「ＮＯ＿３２１５」及び「ＰＫ＿Ｃ」に対し、署名アルゴリズムを施して生成したデータである。

【０１２１】

（５）ＳＡＣの確立１

ここでは、図１３及び図１４に示すフローチャートを用いて、サービス加入、登録時における端末１０と各サーバ装置とにおけるＳＡＣ確立の動作について説明する。なお、ここで説明する動作は、図１０のステップＳ４０２の詳細である。

ここで、Ｇｅｎ（）を鍵生成関数とし、Ｙをシステム固有のパラメータとする。また、鍵生成関数Ｇｅｎ（）は、Ｇｅｎ（Ｘ、Ｇｅｎ（ｙ，Ｚ））＝Ｇｅｎ（ｙ，Ｇｅｎ（Ｘ，Ｚ））の関係を満たすものとする。なお、鍵生成関数は、任意の公知技術で実現可能なため、詳細については省略する。

【０１２２】

先ず、端末１０の制御部１０３は、メモリカード入出力部１０４を介してメモリカード２０から公開鍵証明書Ｃｅｒｔ＿００１０を読み出す（ステップＳ５０１）。端末１０の通信部１０１はネットワーク６０を介して、Ｃｅｒｔ＿００１０をサーバ装置へ送信し、サーバ装置の通信部はＣｅｒｔ＿００１０を受信する（ステップＳ５０２）。サーバ装置は、ＣＡの公開鍵ＰＫ＿ＣＡを用いて公開鍵証明書Ｃｅｒｔ＿００１０に含まれる署名データＳｉｇ＿００１０ＣＡに対して、署名検証アルゴリズムを施して署名検証する（ステップＳ５０３）。なお、サーバ装置は、ＣＡの公開鍵ＰＫ＿ＣＡを既知であるとする。検証結果が失敗の場合（ステップＳ５０４でＮＯ）、サーバ装置は処理を終了する。検証結果が成功の場合（ステップＳ５０４でＹＥＳ）、サーバ装置の制御部は、ＣＲＬ格納部からＣＲＬを読み出し（ステップＳ５０５）、公開鍵証明書Ｃｅｒｔ＿００１０に含まれるＩＤ＿００１０がＣＲＬに登録されているか否かを判断する。

【０１２３】

ＩＤ＿００１０がＣＲＬに登録されていると判断する場合（ステップＳ５０６でＹＥＳ）、サーバ装置は処理を終了する。ＩＤ＿００１０がＣＲＬに登録されていないと判断する場合（ステップＳ５０６でＮＯ）、サーバ装置の制御部は、Ｃｅｒｔ管理部から公開鍵証明書Ｃｅｒｔ＿Ｌを読み出す（ステップＳ５０７）。制御部は、通信部及びネットワーク６０を介して公開鍵証明書Ｃｅｒｔ＿Ｌを端末１０へ送信し、端末１０の通信部は、Ｃｅｒｔ＿Ｌを受信する（ステップＳ５０８）。

【０１２４】

端末１０の制御部１０３は、公開鍵証明書Ｃｅｒｔ＿Ｌを受け取ると、ＣＡの公開鍵ＰＫ＿ＣＡを用いてＣｅｒｔ＿Ｌに含まれる署名データＳｉｇ＿ＬＣＡに対して、署名検証アルゴリズムを施して署名検証する（ステップＳ５０９）。なお、端末１０は、ＣＡの公開鍵ＰＫ＿ＣＡを既知であるとする。検証結果が失敗の場合（ステップＳ５１０でＮＯ）、端末１０は処理を終了する。検証結果が成功の場合（ステップＳ５１０でＹＥＳ）、制御部１０３は、ＣＲＬ格納部１０６からＣＲＬを読み出し（ステップＳ５１１）、公開鍵証明書Ｃｅｒｔ＿Ｌに含まれて受け取ったＩＤ＿ＬがＣＲＬに登録されているか否かを判断する。

【０１２５】

ＩＤ＿ＬがＣＲＬに登録されていると判断する場合（ステップＳ５１２でＹＥＳ）、端末１０は処理を終了する。ＩＤ＿ＬがＣＲＬに登録されていないと判断する場合（ステップＳ５１２でＮＯ）、端末１０は処理を継続する。

ステップＳ５０７の処理に続いて、サーバ装置の公開鍵暗号処理部は、乱数Ｃｈａ＿Ｂを生成する（ステップＳ５１３）。サーバ装置の通信部は、ネットワーク６０を介して乱

数Ｃｈａ＿Ｂを端末１０へ送信し、端末１０の通信部１０１は、乱数Ｃｈａ＿Ｂを受信する（ステップＳ５１４）。

【０１２６】

端末１０の制御部１０３は、乱数Ｃｈａ＿Ｂを受け取ると、メモリカード入出力部１０４を介してメモリカード２０のセキュア領域２０４ａから秘密鍵Ｒ＿００１０を読み出し、読み出した秘密鍵Ｒ＿００１０と先程受け取った乱数Ｃｈａ＿Ｂとを公開鍵暗号処理部１０７へ出力する。公開鍵暗号処理部１０７は、乱数Ｃｈａ＿Ｂに、秘密鍵Ｒ＿００１０を用いて署名生成アルゴリズムを施して署名データＳｉｇ＿ａを生成する（ステップＳ５１５）。通信部１０１は、公開鍵暗号処理部１０７が生成した署名データＳｉｇ＿ａを、ネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部は、署名データＳｉｇ＿ａを受信する（ステップＳ５１６）。

【０１２７】

サーバ装置の公開鍵暗号処理部は、制御部を介して署名データＳｉｇ＿ａを受け取ると、ステップＳ５０２でＣｅｒｔ＿００１０に含んで受け取った公開鍵ＰＫ＿００１０を用いて署名データＳｉｇ＿ａに署名検証アルゴリズムを施して署名検証する（ステップＳ５１７）。検証結果が失敗の場合（ステップＳ５１８でＮＯ）、サーバ装置は処理を終了する。検証結果が成功の場合（ステップＳ５１８でＹＥＳ）、サーバ装置は処理を継続する。

【０１２８】

一方、端末１０は、ステップＳ５１５の処理に続いて、公開鍵暗号処理部１０７において乱数Ｃｈａ＿Ａを生成する（ステップＳ５１９）。公開鍵暗号処理部１０７は、生成した乱数Ｃｈａ＿Ａを、制御部１０３、通信部１０１及びネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部は、乱数Ｃｈａ＿Ａを受信する（ステップＳ５２０）。

【０１２９】

サーバ装置の制御部は、受信した乱数Ｃｈａ＿Ａを公開鍵暗号処理部へ出力し、公開鍵暗号処理部は、受け取った乱数Ｃｈａ＿Ａに、内部に保持している秘密鍵Ｒ＿Ｌを用い、署名アルゴリズムを施して署名データＳｉｇ＿ｂを生成する（ステップＳ５２１）。サーバ装置は、生成した署名データＳｉｇ＿ｂを制御部、通信部及びネットワーク６０を介して端末１０へ送信し、端末１０の通信部１０１は、署名データＳｉｇ＿ｂを受信する（ステップＳ５２２）。

【０１３０】

端末１０の公開鍵暗号処理部１０７は制御部１０３を介して、署名データＳｉｇ＿ｂを受け取ると、ステップＳ５０８でＣｅｒｔ＿Ｌに含んで受け取った公開鍵ＰＫ＿Ｌを用いて署名データＳｉｇ＿ｂに署名検証アルゴリズムを施して署名検証する（ステップＳ５２３）。検証結果が失敗の場合（ステップＳ５２４でＮＯ）、端末１０は処理を終了する。検証結果が成功の場合（ステップＳ５２４でＹＥＳ）、端末１０の公開鍵暗号処理部１０７は、乱数「ａ」を生成し（ステップＳ５２５）、生成した乱数「ａ」を用いてＫｅｙ＿Ａ＝Ｇｅｎ（Ａ，Ｙ）を生成する（ステップＳ５２６）。端末１０の通信部１０１は、公開鍵暗号処理部１０７により生成されたＫｅｙ＿Ａをネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部は、Ｋｅｙ＿Ａを受信する（ステップＳ５２７）。

【０１３１】

サーバ装置の公開鍵暗号処理部は、Ｋｅｙ＿Ａを受け取ると、乱数「ｂ」を生成し（ステップＳ５２８）、生成した乱数「ｂ」を用いてＫｅｙ＿Ｂ＝Ｇｅｎ（Ｂ，Ｙ）を生成する（ステップＳ５２９）。サーバ装置の通信部は、公開鍵暗号処理部により生成されたＫｅｙ＿Ｂをネットワーク６０を介して端末１０へ送信し、端末１０の通信部は、Ｋｅｙ＿Ｂを受信する（ステップＳ５３０）。また、サーバ装置の公開鍵暗号処理部は、ステップＳ５２８で生成した乱数「ｂ」と、ステップＳ５２７で受け取ったＫｅｙ＿Ａとを用いて、Ｋｅｙ＿ＡＢ＝Ｇｅｎ（Ｂ，Ｋｅｙ＿Ａ）＝Ｇｅｎ（Ｂ，Ｇｅｎ（Ａ，Ｙ））を生成し（ステップＳ５３１）、生成したＫｅｙ＿ＡＢをセッション鍵として制御部へ出力する（

ステップＳ５３２）。その後サーバ装置は、図１０のステップＳ４０３に戻って処理を続ける。

【０１３２】

一方、端末１０の公開鍵暗号処理部１０７は、ステップＳ５３０でＫｅｙ＿Ｂを受け取ると、Ｋｅｙ＿ＢとステップＳ５２５で生成した乱数「ａ」とからＫｅｙ＿ＡＢ＝Ｇｅｎ（ａ，Ｋｅｙ＿Ｂ）＝Ｇｅｎ（ａ，Ｇｅｎ（Ｂ，ｙ））を生成し（ステップＳ５３３）、生成したＫｅｙ＿ＡＢをセッション鍵として制御部１０３へ出力する（ステップＳ５３４）。その後端末１０は、図１０のステップＳ４０６に戻って処理を続ける。

【０１３３】

（６）全体の動作２（サービス利用時）

ここでは、図１のフローチャートから続く情報セキュリティシステム１全体の動作について図１５に示すフローチャートを用いて説明する。なお、図１５に示す動作は、情報セキュリティシステム１全体の動作の内、「サービス利用時」における動作である。なお、ここでは、サーバ装置３０、サーバ装置４０及びサーバ装置５０を、単に「サーバ装置」と呼称することがある。

【０１３４】

端末１０において、操作入力部１０２を介してユーザの入力を受け付けることにより、サーバ装置に対するサービス利用要求が発生すると（ステップＳ６０１）、制御部１０３は、メモリカード入出力部１０４を介してメモリカード２０のセキュア領域２０４ａから、ユーザが指定したサーバ装置により発行された公開鍵証明書Ｃｅｒｔ＿Ｎ（Ｎ＝Ａ、Ｂ、又はＣ）を読み出す（ステップＳ６０２）。制御部１０３は、読み出した公開鍵証明書Ｃｅｒｔ＿Ｎを、通信部１０１及びネットワーク６０を介して指定のサーバ装置へ送信し、サーバ装置の通信部は公開鍵証明書Ｃｅｒｔ＿Ｎを受信する（ステップＳ６０３）。

【０１３５】

サーバ装置の制御部は、公開鍵証明書Ｃｅｒｔ＿Ｎを受け取ると、以下に示す様に受け取ったＣｅｒｔ＿Ｎが正しいか否か検証する（ステップＳ６０４）。制御部は、登録情報管理部から端末１０に対応する登録情報を読み出し、受け取ったＣｅｒｔ＿Ｎに含まれるサービスＩＤ、会員番号及び端末１０の公開鍵が登録されている情報と一致するか否か判断する。更に、制御部は、Ｃｅｒｔ＿Ｎに含まれる署名データＳｉｇ＿Ｎを公開鍵暗号処理部に出力する。Ｓｉｇ＿Ｎを受け取った公開鍵暗号処理部は、受け取った署名データＳｉｇ＿Ｎに署名検証アルゴリズムを施してＳｉｇ＿Ｎを検証し、検証結果を制御部へ出力する。

【０１３６】

Ｃｅｒｔ＿Ｎの検証に失敗した場合（ステップＳ６０５でＮＧ）、サーバ装置は処理を終了する。Ｃｅｒｔ＿Ｎの検証に成功した場合（ステップＳ６０５でＯＫ）、サーバ装置と端末１０とは、ＳＡＣを確立する処理を行う（ステップＳ６０６）。

端末１０とＳＡＣを確立すると、サーバ装置の制御部は、コンテンツ格納部からコンテンツを読み出し（ステップＳ６０７）、ステップＳ６０６において端末１０と共有したセッション鍵を暗号鍵として用い、読み出したコンテンツを暗号化する（ステップＳ６０８）。ここで用いる暗号アルゴリズムの一例はＤＥＳである。サーバ装置の通信部は、ネットワーク６０を介して暗号化コンテンツを端末１０へ送信し、端末１０の通信部１０１は、暗号化コンテンツを受信する（ステップＳ６０９）。

【０１３７】

端末１０の制御部１０３は、暗号化コンテンツを受け取ると、ステップＳ６０６においてサーバ装置と共有したセッション鍵を復号鍵として用い、受け取った暗号化コンテンツを復号する（ステップＳ６１０）。制御部１０３は、メモリカード入出力部１０４を介して、復号したコンテンツをメモリカード２０のコンテンツ格納領域２０４ｂに格納する（ステップＳ６１１）。

【０１３８】

（７）ＳＡＣの確立２

ここでは、図１６、図１７及び図１８に示すフローチャートを用いて、サービス利用時における端末１０と各サーバ装置とにおけるＳＡＣ確立処理の動作について説明する。なお、ここで説明する動作は、図１５のステップＳ６０６の詳細である。

ここで、Ｇｅｎ（）を鍵生成関数とし、Ｙをシステム固有のパラメータとする。また、鍵生成関数Ｇｅｎ（）は、Ｇｅｎ（Ｘ、Ｇｅｎ（ｙ，Ｚ））＝Ｇｅｎ（ｙ，Ｇｅｎ（Ｘ，Ｚ））の関係を満たすものとする。

【０１３９】

先ず、端末１０の制御部１０３は、メモリカード入出力部１０４を介してメモリカード２０から公開鍵証明書Ｃｅｒｔ＿００１０を読み出す（ステップＳ７０１）。端末１０の通信部１０１はネットワーク６０を介して、Ｃｅｒｔ＿００１０をサーバ装置へ送信し、サーバ装置の通信部はＣｅｒｔ＿００１０を受信する（ステップＳ７０２）。サーバ装置の公開鍵暗号処理部は、ＣＡの公開鍵ＰＫ＿ＣＡを用いて公開鍵証明書Ｃｅｒｔ＿００１０に含まれる署名データＳｉｇ＿００１０ＣＡに対して、署名検証アルゴリズムを施して署名検証する（ステップＳ７０３）。検証結果が失敗の場合（ステップＳ７０４でＮＯ）、サーバ装置は処理を終了する。検証結果が成功の場合（ステップＳ７０４でＹＥＳ）、サーバ装置の制御部は、ＣＲＬ格納部からＣＲＬを読み出し（ステップＳ７０５）、公開鍵証明書Ｃｅｒｔ＿００１０に含まれるＩＤ＿００１０がＣＲＬに登録されているか否かを判断する。

【０１４０】

ＩＤ＿００１０がＣＲＬに登録されていると判断する場合（ステップＳ７０６でＹＥＳ）、サーバ装置は処理を終了する。ＩＤ＿００１０がＣＲＬに登録されていないと判断する場合（ステップＳ７０６でＮＯ）、サーバ装置の制御部は、Ｃｅｒｔ管理部から公開鍵証明書Ｃｅｒｔ＿Ｌを読み出す（ステップＳ７０７）。制御部は、通信部及びネットワーク６０を介して公開鍵証明書Ｃｅｒｔ＿Ｌを端末１０へ送信し、端末１０の通信部は、Ｃｅｒｔ＿Ｌを受信する（ステップＳ７０８）。

【０１４１】

端末１０の制御部１０３は、公開鍵証明書Ｃｅｒｔ＿Ｌを受け取ると、ＣＡの公開鍵ＰＫ＿ＣＡを用いてＣｅｒｔ＿Ｌに含まれる署名データＳｉｇ＿ＬＣＡに対して、署名検証アルゴリズムを施して署名検証する（ステップＳ７０９）。検証結果が失敗の場合（ステップＳ７１０でＮＯ）、端末１０は処理を終了する。検証結果が成功の場合（ステップＳ７１０でＹＥＳ）、制御部１０３は、ＣＲＬ格納部１０６からＣＲＬを読み出し（ステップＳ７１１）、公開鍵証明書Ｃｅｒｔ＿Ｌに含まれて受け取ったＩＤ＿ＬがＣＲＬに登録されているか否かを判断する。

【０１４２】

ＩＤ＿ＬがＣＲＬに登録されていると判断する場合（ステップＳ７１２でＹＥＳ）、端末１０は処理を終了する。ＩＤ＿ＬがＣＲＬに登録されていないと判断する場合（ステップＳ７１２でＮＯ）、端末１０は処理を継続する。

ステップＳ７０７の処理に続いて、サーバ装置の公開鍵暗号処理部は、乱数Ｃｈａ＿Ｄを生成する（ステップＳ７１３）。サーバ装置の通信部は、ネットワーク６０を介して乱数Ｃｈａ＿Ｄを端末１０へ送信し、端末１０の通信部１０１は、乱数Ｃｈａ＿Ｄを受信する（ステップＳ７１４）。

【０１４３】

端末１０の公開鍵暗号処理部１０７は、Ｃｈａ＿Ｄを受け取ると、

Ｒ１＝（ｒｘ，ｒｙ）＝Ｃｈａ＿Ｄ＊Ｇ

を計算し（ステップＳ７１５）、

Ｓ×Ｃｈａ＿Ｄ＝ｍ＋ｒｘ×ＳＫ　（ｍｏｄ　ｑ）

から、Ｓを計算する（ステップＳ７１６）。ここで、ｑは、楕円曲線Ｅの位数であり、ｍは、端末１０がサーバ装置へ送信するメッセージであり、ＳＫは、メモリカード入出力部１０４を介してメモリカード２０のセキュア領域２０４ａから読み出した端末１０のサービス用秘密鍵である。

【０１４４】
端末１０は、得られたＲ１とＳとから署名データＳｉｇ＿ｄ＝（Ｒ１，Ｓ）を生成し（ステップＳ７１７）、生成した署名データＳｉｇ＿ｄとメッセージｍと共にサーバ装置へ送信し、サーバ装置は署名データＳｉｇ＿ｄとメッセージｍとを受信する（ステップＳ７１８）。
サーバ装置の公開鍵暗号処理部は、
ｍ＊Ｇ＋ｒｘ＊ＰＫ＿Ｎ
を計算し、更に、
Ｓ＊Ｒ１
を計算する（ステップＳ７１９）。
【０１４５】
サーバ装置の公開鍵暗号処理部は、Ｓ＊Ｒ１＝ｍ＊Ｇ＋ｒｘ＊ＰＫ＿Ｎ
が成立するかどうか判定することにより、送信者である端末１０の身元を確認する（ステップＳ７２０）。これは、

$$
\begin{aligned}
S*R1 &= \{((m+rx\times SK)/Cha\_D)\times Cha\_D\}*G \\
&= (m+rx\times SK)*G \\
&= m*G+(rx\times SK)*G \\
&= m*G+rx*PK\_N
\end{aligned}
$$

となることから明らかである。
【０１４６】
Ｓ＊Ｒ１≠ｍ＊Ｇ＋ｒｘ＊ＰＫ＿Ｎの場合（ステップＳ７２０でＮＯ）、サーバ装置は処理を終了する。Ｓ＊Ｒ１＝ｍ＊Ｇ＋ｒｘ＊ＰＫ＿Ｎの場合（ステップＳ７２０でＹＥＳ）、サーバ装置は、処理を続ける。
一方で、端末１０は、ステップＳ７１８においてＳｉｇ＿ｄ及びｍをサーバ装置へ送信した後、公開鍵暗号処理部１０７は、乱数Ｃｈａ＿Ｅを生成し（ステップＳ７２１）、生成した乱数Ｃｈａ＿Ｅを制御部１０３、通信部１０１ネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部はＣｈａ＿Ｅを受信する（ステップＳ７２２）。
【０１４７】
サーバ装置の公開鍵暗号処理部は、制御部を介して乱数Ｃｈａ＿Ｅを受け取ると、
Ｒ２＝（ｒｘ，ｒｙ）＝Ｃｈａ＿Ｅ＊Ｇ
を計算し（ステップＳ７２３）、
Ｓ´×Ｃｈａ＿Ｅ＝ｍ´＋ｒｘ×Ｋｓ＿Ｍ　（ｍｏｄ　ｑ）
から、Ｓ´を計算する（ステップＳ７２４）。ここで、ｍ´は、サーバ装置が端末１０へ送信するメッセージであり、Ｋｓ＿Ｍ（Ｍ＝３０、４０、又は５０）は、サーバ装置の秘密鍵である。より具体的に、Ｋｓ＿３０は、サーバ装置３０の秘密鍵であり、Ｋｓ＿４０は、サーバ装置４０の秘密鍵であり、Ｋｓ＿５０は、サーバ装置５０の秘密鍵である。
【０１４８】
サーバ装置は、得られたＲ２とＳ´とから、署名データＳｉｇ＿ｅ＝（Ｒ２，Ｓ´）を生成し（ステップＳ７２５）、生成した署名データＳｉｇ＿ｅをメッセージｍ´と共に端末１０へ送信し、端末１０は署名データＳｉｇ＿ｅとメッセージｍ´とを受信する（ステップＳ７２６）。
端末１０の公開鍵暗号処理部１０７は、
ｍ´＊Ｇ＋ｒｘ＊Ｋｐ＿Ｍ
を計算する（ステップＳ７３１）。ここで、Ｋｐ＿Ｍ（Ｍ＝３０、４０、又は５０）は、Ｋｐ＿Ｍ＝Ｋｓ＿Ｍ＊Ｇを計算することにより生成された各サーバ装置の公開鍵である。より具体的に、Ｋｐ＿３０は、サーバ装置３０の公開鍵であり、Ｋｓ＿３０に対応している。Ｋｐ＿４０は、サーバ装置４０の公開鍵であり、秘密鍵Ｋｓ＿４０に対応している。Ｋｐ＿５０は、サーバ装置５０の公開鍵であり、秘密鍵Ｋｓ＿５０に対応している。
【０１４９】
公開鍵暗号処理部１０７は、更に、

Ｓ′＊Ｒ２
を計算する（ステップＳ７３１）。
公開鍵暗号処理部１０７は、Ｓ′＊Ｒ２＝ｍ′＊Ｇ＋ｒｘ＊Ｋｐ＿Ｍ
が成立するかどうか判定することにより、送信者である端末１０の身元を確認する（ステップＳ７３２）。これは、

Ｓ′＊Ｒ２＝｛（（ｍ′＋ｒｘ×Ｋｓ＿Ｍ）／Ｃｈａ＿Ｅ）×Ｃｈａ＿Ｅ｝＊Ｇ
＝（ｍ′＋ｒｘ×Ｋｓ＿Ｍ）＊Ｇ
＝ｍ′＊Ｇ＋（ｒｘ×Ｋｓ＿Ｍ）＊Ｇ
＝ｍ′＊Ｇ＋ｒｘ＊Ｋｐ＿Ｍ

となることから明らかである。

【０１５０】

Ｓ′＊Ｒ２≠ｍ′＊Ｇ＋ｒｘ＊Ｋｐ＿Ｍの場合（ステップＳ７３２でＮＯ）、端末１０は処理を終了する。Ｓ′＊Ｒ２＝ｍ＊Ｇ＋ｒｘ＊Ｋｐ＿Ｍの場合（ステップＳ７３２でＹＥＳ）、公開鍵暗号処理部１０７は、乱数「ｄ」を生成し（ステップＳ７３３）、生成した乱数「ｄ」を用いてＫｅｙ＿Ｄ＝Ｇｅｎ（Ｄ，Ｙ）を生成する（ステップＳ７３４）。端末１０の通信部１０１は、公開鍵暗号処理部１０７により生成されたＫｅｙ＿Ｄをネットワーク６０を介してサーバ装置へ送信し、サーバ装置の通信部は、Ｋｅｙ＿Ｄを受信する（ステップＳ７３５）。

【０１５１】

サーバ装置の公開鍵暗号処理部は、Ｋｅｙ＿Ｄを受け取ると、乱数「ｅ」を生成し（ステップＳ７３６）、生成した乱数「ｅ」を用いてＫｅｙ＿Ｅ＝Ｇｅｎ（Ｅ，Ｙ）を生成する（ステップＳ７３７）。サーバ装置の通信部は、公開鍵暗号処理部により生成されたＫｅｙ＿Ｅをネットワーク６０を介して端末１０へ送信し、端末１０の通信部は、Ｋｅｙ＿Ｅを受信する（ステップＳ７３８）。また、サーバ装置の公開鍵暗号処理部は、ステップＳ７３５で生成した乱数「ｅ」と、ステップＳ７３５で受け取ったＫｅｙ＿Ｄとを用いて、Ｋｅｙ＿ＤＥ＝Ｇｅｎ（ｅ，Ｋｅｙ＿Ｄ）＝Ｇｅｎ（ｅ，Ｇｅｎ（Ｄ，Ｙ））を生成し（ステップＳ７４１）、生成したＫｅｙ＿ＤＥをセッション鍵として制御部へ出力する（ステップＳ７４２）。その後サーバ装置は、図１５のステップＳ６０７に戻って処理を続ける。

【０１５２】

一方、端末１０の公開鍵暗号処理部１０７は、ステップＳ７３８でＫｅｙ＿Ｅを受け取ると、Ｋｅｙ＿ＥとステップＳ７３３で生成した乱数「ｄ」とからＫｅｙ＿ＤＥ＝Ｇｅｎ（ｄ，Ｋｅｙ＿Ｅ）＝Ｇｅｎ（ｄ，Ｇｅｎ（Ｅ，Ｙ））を生成し（ステップＳ７３９）、生成したＫｅｙ＿ＤＥをセッション鍵として制御部１０３へ出力する（ステップＳ７４０）。その後端末１０は、図１５のステップＳ６１０に戻って処理を続ける。

【０１５３】

（７）楕円曲線のシステムパラメータ生成処理の動作

情報セキュリティシステム１において、認証局（ＣＡ）は、各機器に公開鍵証明書を発行する機能、及び、暗号に適したシステムパラメータを生成し、生成したシステムパラメータを各サーバ装置へ通知する機能を有する。ここで、システムパラメータは、楕円曲線Ｅ：$y^2=x^3+ax+b$を構成するａ、ｂ、素数ｐ、ｐの位数ｑ、及び、楕円曲線Ｅ上のベースポイントＧを指す。特に、当該システムにおいて、ＣＡは、サーバ装置毎に固有のシステムパラメータを生成する。

【０１５４】

ここでは、図１９に示すフローチャートを用いて、ＣＡによる楕円曲線のシステムパラメータ生成処理の動作について説明する。

ＣＡが有する楕円曲線管理装置は、乱数を生成し（ステップＳ８０１）、生成した乱数を用いて楕円曲線を決定するａ、ｂ、素数ｐ及び元Ｇを生成し、（ステップＳ８０２）、生成したパラメータを用いて、楕円曲線の位数を計算する（ステップＳ８０３）。

【０１５５】

次に、計算された位数を用いて、以下に示す安全な楕円曲線の条件を満たすか否かを判定することにより、楕円曲線の安全性を判定する。

現存するすべての解読法に対して安全な楕円曲線の条件は、有限体ＧＦ（ｐ）上の楕円曲線の場合、

（条件１）楕円曲線の位数がｐ－１、ｐ及びｐ＋１のいずれでもないこと、及び

（条件２）この楕円曲線の位数が大きい素因数をもつことである。

【０１５６】

「暗号・ゼロ知識証明、数論」（１５５ページ～１５６ページ、情報処理学会監修、岡本龍明・太田和夫共編、共立出版、１９９５年）によると、これらの条件を満たす場合に、解読するために必要な計算時間は、前記位数の最大素因数に関する指数関数時間である。

（条件１）及び（条件２）を満たさない場合（ステップＳ８０４でＮＧ）、ステップＳ８０１に戻り、乱数の生成と、楕円曲線のシステムパラメータの生成と、楕円曲線の位数の計算と、条件判定とを繰り返す。

【０１５７】

（条件１）及び（条件２）を満たす場合（ステップＳ８０４でＯＫ）、楕円曲線管理装置は、生成されたシステムパラメータを、既に生成され、記憶されているシステムパラメータと比較する（ステップＳ８０５）。生成されたシステムパラメータの組み合わせが、記憶されているシステムパラメータの組み合わせの何れかと一致する場合（ステップＳ８０６でＹＥＳ）、生成したシステムパラメータを破棄し（ステップＳ８０７）、ステップＳ８０１に戻り処理を続ける。

【０１５８】

生成されたシステムパラメータの組み合わせが、記憶されているシステムパラメータの組み合わせの何れとも一致しない場合（ステップＳ８０６でＮＯ）、生成されたシステムパラメータの組み合わせを記憶すると共に、サーバ装置３０、サーバ装置４０、又はサーバ装置５０へ送信する（ステップＳ８０８）。

なお、ＣＡが有する楕円曲線管理装置は、サーバ装置３０、サーバ装置４０、及び、サーバ装置５０から要求を受ける毎に、上記の処理を行うものとする。

【０１５９】

これにより、サーバ装置３０、サーバ装置４０、及びサーバ装置５０は、他のサーバ装置と異なるユニークな楕円曲線のシステムパラメータの組み合わせを取得する。

＜まとめ＞

以上説明したように、本発明は、ＳＡＣで利用する公開鍵暗号を、一例として楕円曲線暗号であると想定する。楕円曲線暗号では、秘密鍵を生成してから公開鍵を算出するが、公開鍵の算出には、秘密鍵とシステムパラメータとを利用するため、秘密鍵が共通であっても、システムパラメータが異なれば、異なる公開鍵が算出される。

【０１６０】

そこで、本発明は、コンテンツ配信サービスを提供するサーバ装置が、自身のサービス用のシステムパラメータを、サービス利用者である端末へ送信する。このとき、コンテンツ配信サービスを提供するサーバ装置が複数存在する場合、端末は、複数のサーバ装置から、それぞれ異なるシステムパラメータを取得するものとする。

端末は、既に保持している秘密鍵と受信したパラメータとから公開鍵を算出し、算出した公開鍵をサーバ装置へ返信する。公開鍵を受信したサーバ装置は、公開鍵に対して署名を付与した公開鍵証明書を生成して、端末へ返送する。

【０１６１】

＜その他の変形例＞

以上、本発明を上記実施の形態に基づき説明してきたが、本発明は上記実施の形態に限定されないのは勿論であり、以下の様な場合も本発明に含まれる。

（１）上記実施の形態では、端末１０が各サーバ装置から取得する楕円曲線のシステムパラメータ「ａ、ｂ、ｐ、ｑ、及び、Ｇ」の内、ベースポイントＧがサーバ装置毎に異な

る構成を有しているが、本発明は、この構成に限定されないのは勿論である。端末１０が各サーバ装置から取得するシステムパラメータ「ａ、ｂ、ｐ、ｑ、及び、Ｇ」の内、少なくとも、素数ｐ又はベースポイントＧの何れかが、サーバ装置毎に異なっていればよい。勿論、システムパラメータの各値が、サーバ装置毎に全て異なっている場合も本発明に含まれる。本発明において、端末１０が取得する楕円曲線のシステムパラメータの組み合わせがサーバ装置毎に異なるのは、サーバ装置毎に異なる公開鍵を生成することが目的であり、システムパラメータ自体が異なることは目的ではない。

【０１６２】

（２）上記実施の形態では、端末１０が秘密鍵ＳＫとパラメータとから公開鍵Ｐ＿Ａ、ＰＫ＿Ｂ、及び、ＰＫ＿Ｃを生成する構成を有しているが、公開鍵は必ずしも端末１０で生成される必要はなく、以下の様な場合も本発明に含まれる。

（ａ）サーバ装置が公開鍵を生成する

先ず、端末と各サーバ装置との間でＳＡＣを確立する。

【０１６３】

端末１０は、サービス用秘密鍵ＳＫを生成し、生成したサービス用秘密鍵ＳＫを、ＳＡＣを介して安全かつ確実に各サーバ装置へ送信する。

各サーバ装置は、端末１０のサービス用秘密鍵ＳＫとＣＡから取得した楕円曲線のシステムパラメータとから、秘密鍵ＳＫに対応する公開鍵を生成する。各サーバ装置は、生成した公開鍵に自身の署名を付加した公開鍵証明書を生成し、生成した公開鍵証明書を端末１０へ返信する。

【０１６４】

（ｂ）認証局（ＣＡ）が公開鍵を生成する

先ず、端末１０とＣＡとの間でＳＡＣを確立する。

ＣＡは、異なる３組のシステムパラメータを生成する。端末１０は、サービス用秘密鍵ＳＫを生成し、生成したサービス用秘密鍵ＳＫをＳＡＣを介して安全かつ確実にＣＡへ送信する。

【０１６５】

ＣＡは、端末１０から秘密鍵ＳＫを受信すると、１個の秘密鍵ＳＫと３組のシステムパラメータとから、異なる３個の公開鍵を生成する。ＣＡは、生成した３個の公開鍵を端末へ送信する。

端末１０は、３個の公開鍵を受信すると、それぞれサーバ装置３０、サーバ装置４０及びサーバ装置５０へ送信する。各サーバ装置は、端末１０から公開鍵を受信すると、受信した公開鍵に署名を付加して公開鍵証明書を生成し、生成した公開鍵証明書を端末１０へ返信する。

【０１６６】

（３）ＳＡＣ確立時の署名データ生成及び署名データ検証に用いる公開鍵暗号は、楕円曲線暗号に限定されない。公開鍵暗号としてＲＳＡ暗号を用いる構成も本発明に含まれる。ここでは、ＲＳＡ暗号を用いた実施形態について以下に述べる。

（ＲＳＡ暗号の基礎的事項）

公開鍵：Ｎ、ｅ

秘密鍵：Ｐ、Ｑ、ｄ

$N=P\times Q$、$(e,(P-1)(Q-1))=1$

$ed\equiv 1 \bmod (P-1)(Q-1)$

暗号化：　$C=E(M)=M^e \bmod N$

復号　：　$M=D(C)=C^d \bmod N$

（動作）

端末１０が、サーバ装置３０、サーバ装置４０及びサーバ装置５０から公開鍵証明書の発行を受ける処理の動作について以下に述べる。

【０１６７】

（ステップ１）端末１０は、任意の相違なる二つの大きな素数P_1、Q_1を選ぶ。また、

端末１０は、乱数生成器などにより、秘密鍵ｄを生成する。
（ステップ２）端末１０は、$N_1 = P_1 \times Q_1$を計算する。また、端末１０は、$e_1 d \equiv 1 \bmod (P_1 - 1)(Q_1 - 1)$から、$e_1$を計算する。
（ステップ３）端末１０は、公開鍵（N_1、e_1）を、サーバ装置３０へ送信し、サーバ装置３０から公開鍵証明書を受信し、記憶する。
【０１６８】
（ステップ４）端末１０は、P_1及びQ_1を削除し、秘密鍵ｄをセキュアな記憶領域に記憶する。
（ステップ５）端末１０は、P_1、Q_1とは異なる大きな素数P_2及びQ_2を選ぶ。
（ステップ６）端末１０は、$N_2 = P_2 \times Q_2$を計算する。また、端末１０は、$e_2 d \equiv 1 \bmod (P_2 - 1)(Q_2 - 1)$から、$e_2$を計算する。
【０１６９】
（ステップ７）端末１０は、公開鍵（N_2、e_2）を、サーバ装置４０へ送信し、サーバ装置４０から公開鍵証明書を受信し、記憶する。
（ステップ８）端末１０は、P_2及びQ_2を削除する。
（ステップ９）端末１０は、P_1、Q_1、P_2、Q_2とは異なる大きな素数P_3及びQ_3を選ぶ。
【０１７０】
（ステップ１０）端末１０は、$N_3 = P_3 \times Q_3$を計算する。また、端末１０は、$e_3 d \equiv 1 \bmod (P_3 - 1)(Q_3 - 1)$から、$e_3$を計算する。
（ステップ１１）端末１０は、公開鍵（N_3、e_3）を、サーバ装置５０へ送信し、サーバ装置５０から公開鍵証明書を受信し、記憶する。
（ステップ１２）端末１０は、P_3及びQ_3を削除する。
【０１７１】
この様に、端末１０は、楕円曲線のシステムパラメータに替えて、大きな素数の組（Ｐ、Ｑ）を複数個生成するか、又は、取得し、１個の秘密鍵ｄと複数個の素数の組（Ｐ、Ｑ）とから、ＲＳＡ暗号のアルゴリズムに従い、複数個の公開鍵（Ｎ、ｅ）を生成することができる。即ち、端末１０は、楕円曲線暗号のみならず、ＲＳＡ暗号を用いても、１個の秘密鍵から複数個の公開鍵を生成し、生成した複数個の公開鍵を用いて、複数のサーバ装置とＳＡＣを確立し、コンテンツの送受信を行うことができる。
【０１７２】
（４）上記のＲＳＡ暗号を用いた変形例では、端末１０が複数個の公開鍵を生成するのでなく、各サーバ装置が公開鍵を生成するように構成されてもよい。
（５）端末１０及び各サーバ装置は、ＣＲＬをネットワーク６０を介してＣＡより受信する構成を有しているが、ＣＲＬの取得方法はこれに限定されない。放送で受信してもよいし、ＤＶＤ等の記録媒体に格納して配布されてもよい。
【０１７３】
（６）メモリカードに秘密鍵、公開鍵、コンテンツを格納しなくても端末内部の記憶領域に格納してもよい。このとき、少なくとも秘密鍵はセキュアな記憶領域に格納されるべきである。
（７）上記実施の形態では、端末１０が、秘密鍵及び公開鍵の生成処理、ＳＡＣ確立処理の機能を担っているが、本発明は、端末１０がこれらの処理を行うことは必須ではなく、ネットワークに接続された端末に挿入されたＩＣチップを備えるメモリカード（以下、「ＩＣメモリカード」と呼称する）が、秘密鍵及び公開鍵の生成処理、ＳＡＣ確立処理等を行う場合も本発明に含まれる。
【０１７４】
以下では、ＩＣメモリカードを用いた実施形態について説明する。
ＩＣメモリカードは、端末に挿入されており、端末を介してサーバ装置３０、サーバ装置４０及びサーバ装置５０、並びに、ＣＡと通信可能であるとする。
ＩＣメモリカードは、ＩＣチップ、ＲＯＭ、ＲＡＭなどから構成される制御部と、記憶

領域とから構成される。なお、記憶領域の一部は外部から解読及び改竄が不可能なセキュア領域であるとする。

【０１７５】

ＩＣメモリカードは、予め、端末を介してＣＡと通信を行い、ＣＡから、ＩＣメモリカードのデバイスＩＤとＩＣメモリカードの公開鍵とＣＡによる署名データとを含む公開鍵証明書の発行を受け、受信した公開鍵証明書を記憶領域に格納している。

更に、ＩＣメモリカードは、サーバ装置３０が公開している公開鍵、サーバ４０が公開している公開鍵、及び、サーバ装置５０が公開している公開鍵を記憶領域に格納している。

【０１７６】

（サービス加入要求）

ここでは、ＩＣメモリカードが、サーバ装置３０に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、公開鍵暗号のアルゴリズムとしてＲＳＡ暗号を用い、サーバ装置３０とＳＡＣを確立する。ＳＡＣ確立の詳細は、上記実施の形態におけるＳＡＣ確立処理と同様であって、上記実施の形態において、端末１０が行っていた処理を、ＩＣメモリカードが行う。

【０１７７】

制御部は、サーバ装置３０との間で確立されたＳＡＣを用い、端末を介してサーバ装置３０から、楕円曲線のシステムパラメータ「a_1、b_1、p_1、q_1、及び、G_1」を受け取る。

制御部は、サービス用秘密鍵を生成し、生成したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、生成したサービス用秘密鍵をセキュア領域に書き込み、算出した公開鍵を、サーバ装置３０との間で確立されたＳＡＣを用い、端末を介してサーバ装置３０へ送信する。その後、制御部は、端末を介してサーバ装置３０から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

【０１７８】

次に、ＩＣメモリカードが、サーバ装置４０に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、サーバ装置４０とＳＡＣを確立し、確立されたＳＡＣを用い、端末を介してサーバ装置４０から、楕円曲線のシステムパラメータ「a_2、b_2、p_2、q_2、及び、G_2」を受け取る。

【０１７９】

制御部は、セキュア領域からサービス用秘密鍵を読み出し、読み出したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、算出した公開鍵を、サーバ装置４０との間で確立されたＳＡＣを用い、端末を介してサーバ装置４０へ送信する。その後、制御部は、端末を介してサーバ装置４０から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

【０１８０】

次に、ＩＣメモリカードが、サーバ装置５０に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、サーバ装置５０とＳＡＣを確立し、確立されたＳＡＣを用い、端末を介してサーバ装置５０から、楕円曲線のシステムパラメータ「a_3、b_3、p_3、q_3、及び、G_3」を受け取る。

【０１８１】

制御部は、セキュア領域からサービス用秘密鍵を読み出し、読み出したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、算出した公開鍵を、サーバ装置５０との間で確立されたＳＡＣを用い、端末を介してサーバ装置５０へ送信する。その後、制御部は、端末を介してサーバ装置５０から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

【０１８２】
この様に、ＩＣメモリカードはサーバ装置３０に対するサービス加入要求時に生成した１個のサービス用秘密鍵と、各サーバ装置から受信したシステムパラメータとを用いて、各サーバ装置に対応する３個の異なる公開鍵を生成することが出来る。
（サービス利用要求）
ここでは、ＩＣメモリカードが、サーバ装置３０に対してサービスの利用を要求するときの制御部の処理について説明する。
【０１８３】
制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置３０から発行されたもの）、及び、サーバ装置３０の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置３０とＳＡＣを確立する。ＳＡＣ確立の詳細は、上記実施の形態におけるＳＡＣ確立処理と同様であって、上記実施の形態において、端末１０が行っていた処理を、ＩＣメモリカードが行う。なお、ここで行うＳＡＣ確立処理の公開鍵暗号のアルゴリズムには、楕円曲線暗号を用いるとする。
【０１８４】
制御部は、サーバ装置３０との間で確立されたＳＡＣを用いて、端末を介してサーバ装置３０から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。
次に、ＩＣメモリカードが、サーバ装置４０に対してサービスの利用を要求するときの制御部の処理について説明する。　制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置４０から発行されたもの）、及び、サーバ装置４０の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置４０とＳＡＣを確立する。
【０１８５】
制御部は、サーバ装置４０との間で確立されたＳＡＣを用いて、端末を介してサーバ装置４０から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。
次に、ＩＣメモリカードが、サーバ装置５０に対してサービスの利用を要求するときの制御部の処理について説明する。　制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置５０から発行されたもの）、及び、サーバ装置５０の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置５０とＳＡＣを確立する。
【０１８６】
制御部は、サーバ装置５０との間で確立されたＳＡＣを用いて、端末を介してサーバ装置５０から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。
この様に、サーバ装置３０、４０、及び５０から取得した各コンテンツは、当該ＩＣメモリカードが挿入されている端末や、その他の端末により再生可能である。
【０１８７】
（８）上記実施の形態では、ＣＡがサーバ装置毎に異なるシステムパラメータを生成し、生成したシステムパラメータを、各サーバ装置へ送信する構成を有しているが、本発明において、サーバ装置は、必ずしもＣＡなどの外部からシステムパラメータを取得する必要はなく、サーバ装置自身がシステムパラメータを生成する構成であってもよい。
サーバ装置自身がシステムパラメータを生成する場合、サーバ装置毎に（業者毎に）異なる公開鍵が端末１０で生成されるために、例えば、サーバ装置毎に異なるＩＤを割り当てて、各サーバ装置は、割り当てられたＩＤに基づきシステムパラメータを生成するように構成してもよい。
【０１８８】
（９）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。
また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読

み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１８９】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１９０】

また、前記プログラム又は前記ディジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記ディジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（１０）上記実施の形態及び上記変形例をそれぞれ組み合わせる構成も本発明に含まれる。

【産業上の利用可能性】

【０１９１】

上記において説明した情報セキュリティシステムは、映画、音楽などのディジタル化された著作物を、放送やネットワークなどを介して流通させる産業において、ユーザが複数のサービス業者を利用する仕組みとして利用できる。

【図面の簡単な説明】

【０１９２】

【図１】情報セキュリティシステム１の構成を示す図である。

【図２】端末１０の構成を機能的に示す機能ブロック図である。

【図３】（ａ）パスワードテーブル１２０のデータ構成を示す図である。（ｂ）ＣＲＬ１３０のデータ構成を示す図である。

【図４】メモリカード２０の構成を機能的に示す機能ブロック図である。

【図５】サーバ装置３０の構成を機能的に示す機能ブロック図である。

【図６】情報セキュリティシステム１全体の動作を示すフローチャートであり、図１５に続く。

【図７】端末１０におけるメモリカード２０の認証処理の動作を示すフローチャートである。

【図８】認証局（ＣＡ）と各機器（端末１０、サーバ装置３０、サーバ装置４０及びサーバ装置５０）とにおける公開鍵証明書発行処理の動作を示すフローチャートである。

【図９】（ａ）公開鍵証明書１４０（Ｃｅｒｔ＿００１０）のデータ構成を示す図である。（ｂ）公開鍵証明書１５０（Ｃｅｒｔ＿００３０）のデータ構成を示す図である。（ｃ）公開鍵証明書１６０（Ｃｅｒｔ＿００４０）のデータ構成を示す図である。（ｄ）公開鍵証明書１７０（Ｃｅｒｔ＿００５０）のデータ構成を示す図である。

【図１０】端末１０と各サーバ装置とにおけるサービス加入、登録処理の動作を示すフローチャートであり、図１１に続く。

【図１１】端末１０と各サーバ装置とにおけるサービス加入、登録処理の動作を示すフローチャートであり、図１０から続く。

【図１２】（ａ）端末１０がサーバ装置３０から発行される公開鍵証明書２１０（Ｃｅｒｔ＿Ａ）のデータ構成を示す図である。（ｂ）端末１０がサーバ装置４０から発行される公開鍵証明書２２０（Ｃｅｒｔ＿Ｂ）のデータ構成を示す図である。（ｃ）端末１０がサーバ装置５０から発行される公開鍵証明書２３０（Ｃｅｒｔ＿Ｃ）のデータ構成を示す図である。

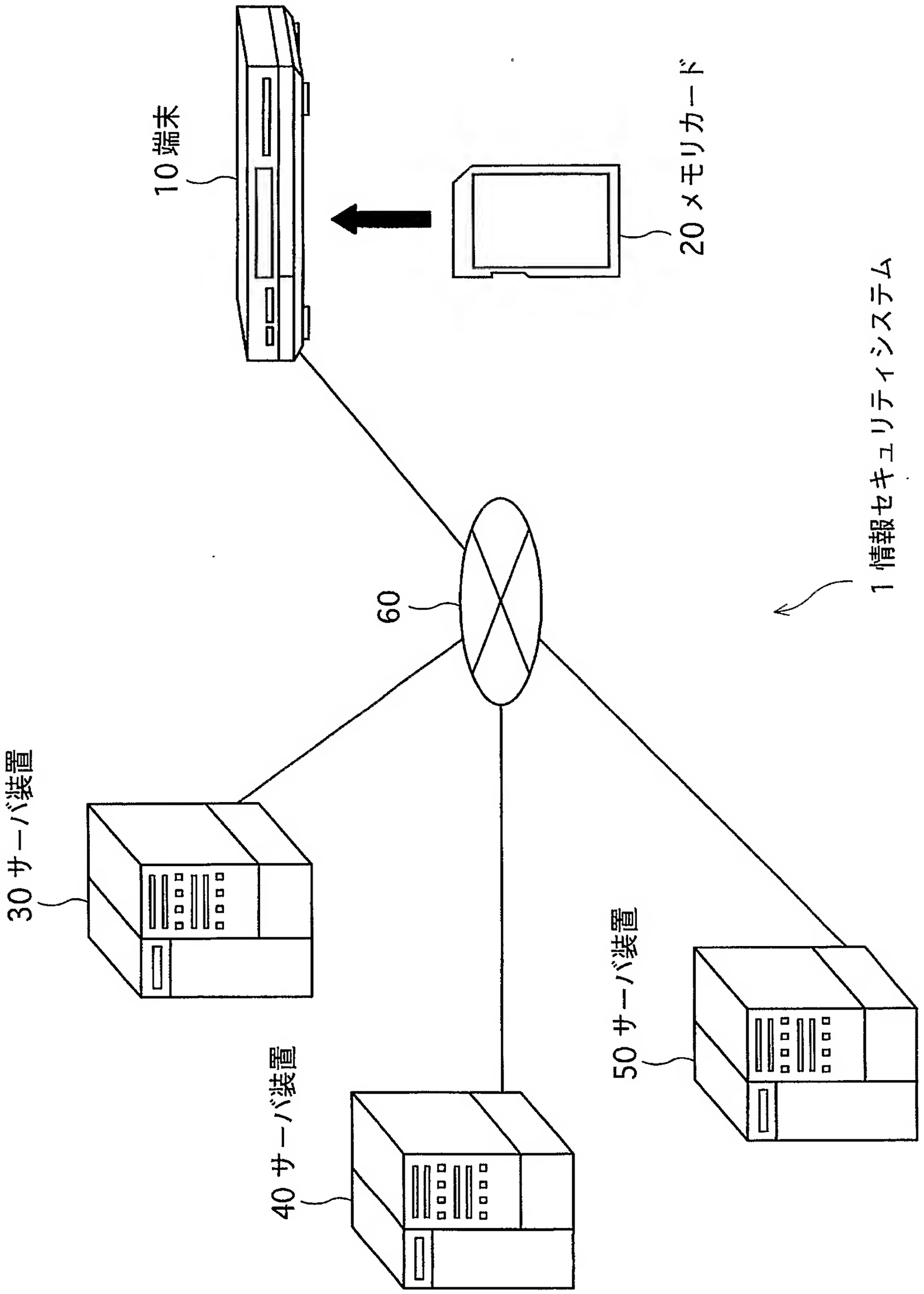
【図１３】端末１０と各サーバ装置とにおける、サービス加入、登録時のＳＡＣ確立処理の動作を示すフローチャートであり、図１４に続く。
【図１４】端末１０と各サーバ装置とにおける、サービス加入、登録時のＳＡＣ確立処理の動作を示すフローチャートであり、図１３から続く。
【図１５】情報セキュリティシステム１全体の動作を示すフローチャートであり、図６から続く。
【図１６】端末１０と各サーバ装置とにおける、サービス利用時のＳＡＣ確立処理の動作を示すフローチャートであり、図１７に続く。
【図１７】端末１０と各サーバ装置とにおける、サービス利用時のＳＡＣ確立処理の動作を示すフローチャートであり、図１６から続き、図１８へ続く。
【図１８】端末１０と各サーバ装置とにおける、サービス利用時のＳＡＣ確立処理の動作を示すフローチャートであり、図１７から続く。
【図１９】認証局における楕円曲線のシステムパラメータ生成の動作を示すフローチャートである。

【符号の説明】

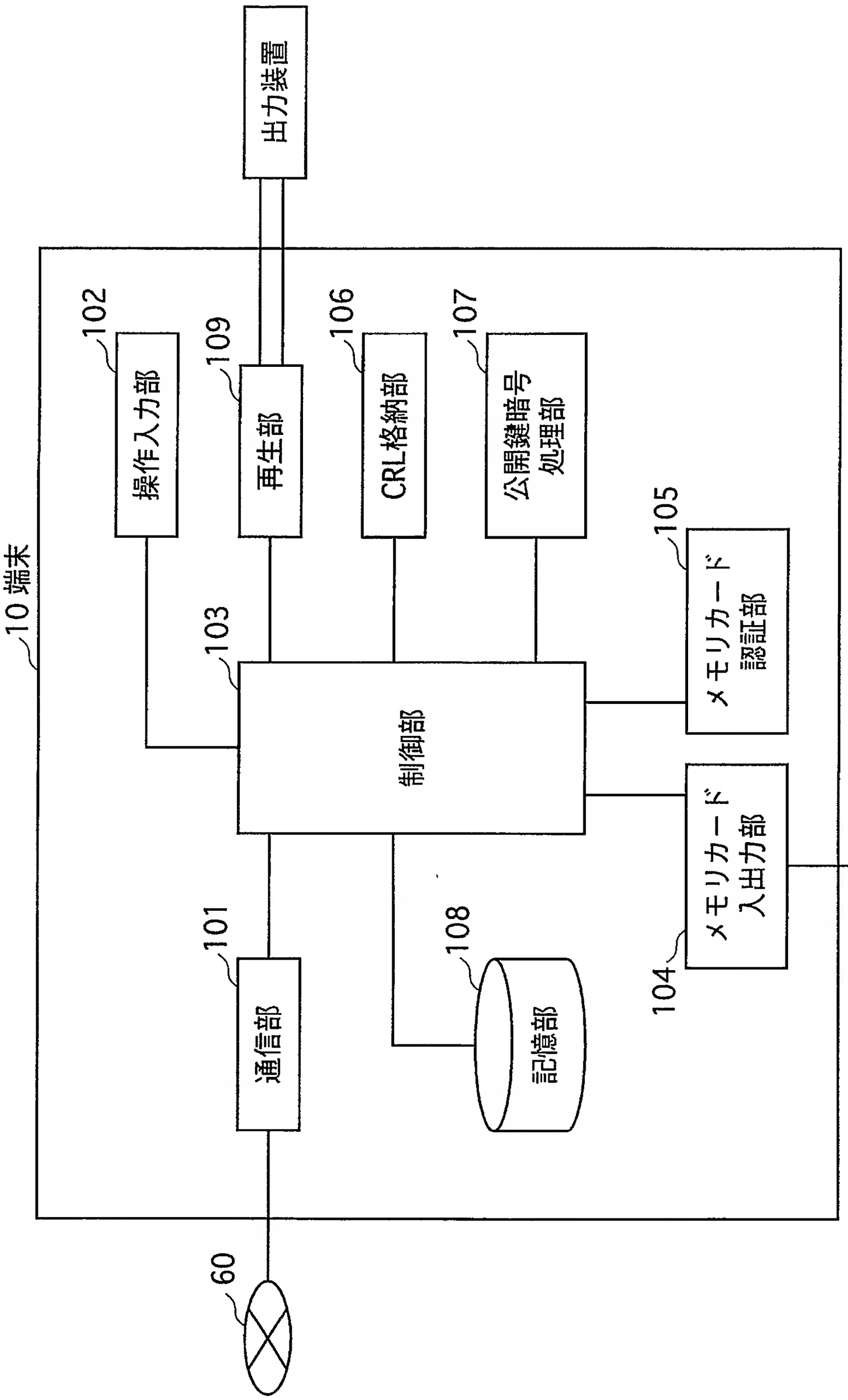
【０１９３】

１	情報セキュリティシステム
１０	端末
２０	メモリカード
３０	サーバ装置
４０	サーバ装置
５０	サーバ装置
６０	ネットワーク
１０１	通信部
１０２	操作入力部
１０３	制御部
１０４	メモリカード入出力部
１０５	メモリカード認証部
１０６	ＣＲＬ格納部
１０７	公開鍵暗号処理部
１０８	記憶部
１０９	再生部
２０１	入出力部
２０２	メモリ制御部
２０３	認証部
２０４	メモリ
２０４ａ	セキュア領域
２０４ｂ	コンテンツ格納領域
２０４ｃ	公開鍵格納領域
３０１	通信部
３０２	制御部
３０３	ＣＲＬ格納部
３０４	Ｃｅｒｔ管理部
３０５	登録情報管理部
３０６	公開鍵暗号処理部
３０７	コンテンツ格納部

【書類名】図面
【図１】



【図２】


出力装置
10 端末
101 通信部
102 操作入力部
103 制御部
104 メモリカード入出力部
105 メモリカード認証部
106 CRL格納部
107 公開鍵暗号処理部
108 記憶部
109 再生部
メモリカード20
60

【図３】

(a)

120 パスワードテーブル

メモリカード番号	認証用パスワード
20	PW_0
21	PW_1
⋮	⋮

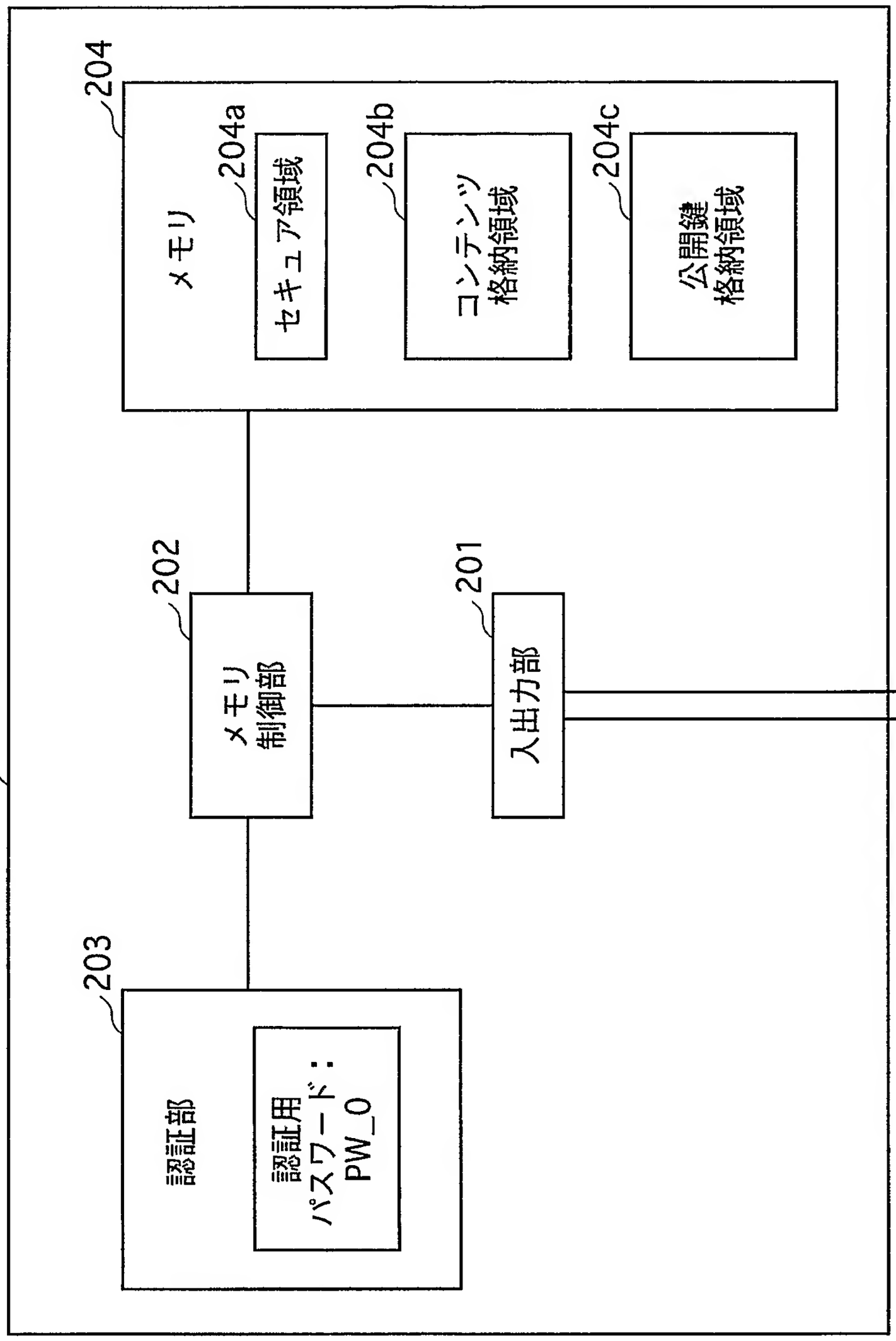
121

(b)

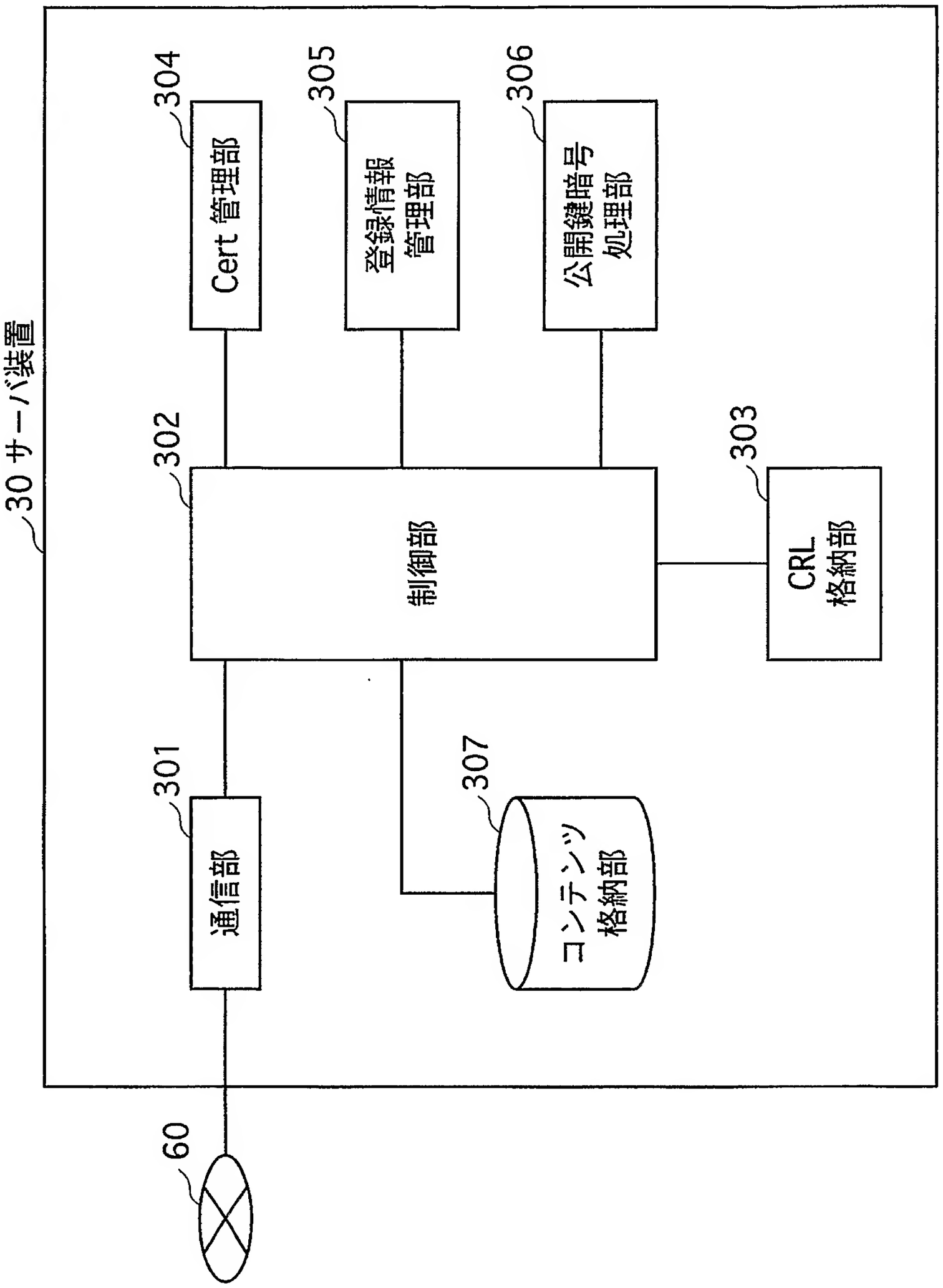
130 CRL

無効化された機器のID
ID_0012
ID_0058
ID_0379
⋮

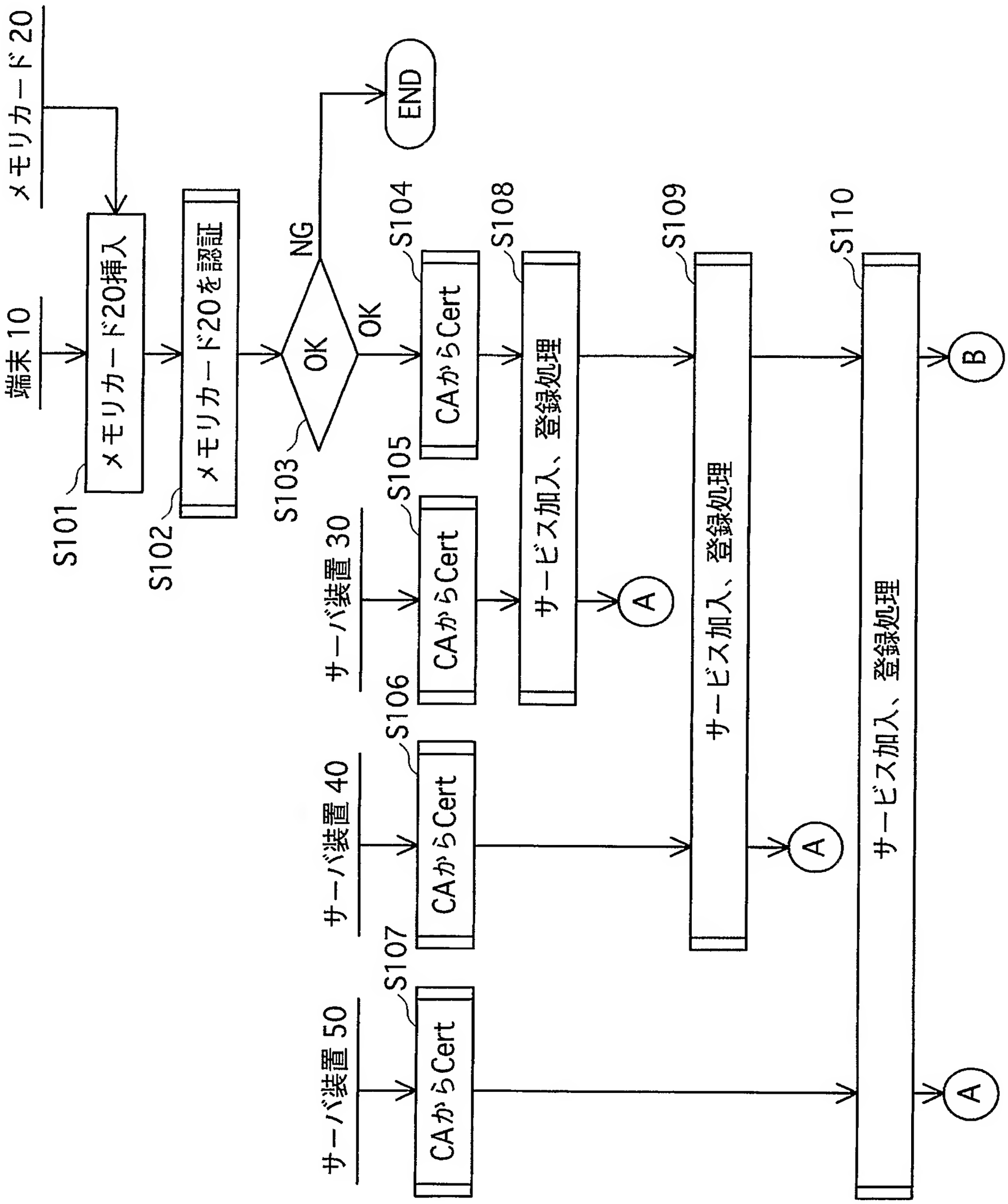
【図４】


20 メモリカード
204
メモリ
204a
セキュア領域
204b
コンテンツ
格納領域
204c
公開鍵
格納領域
202
メモリ
制御部
201
入出力部
端末10の
メモリカード入出力部 105
203
認証部
認証用
パスワード：
PW_0

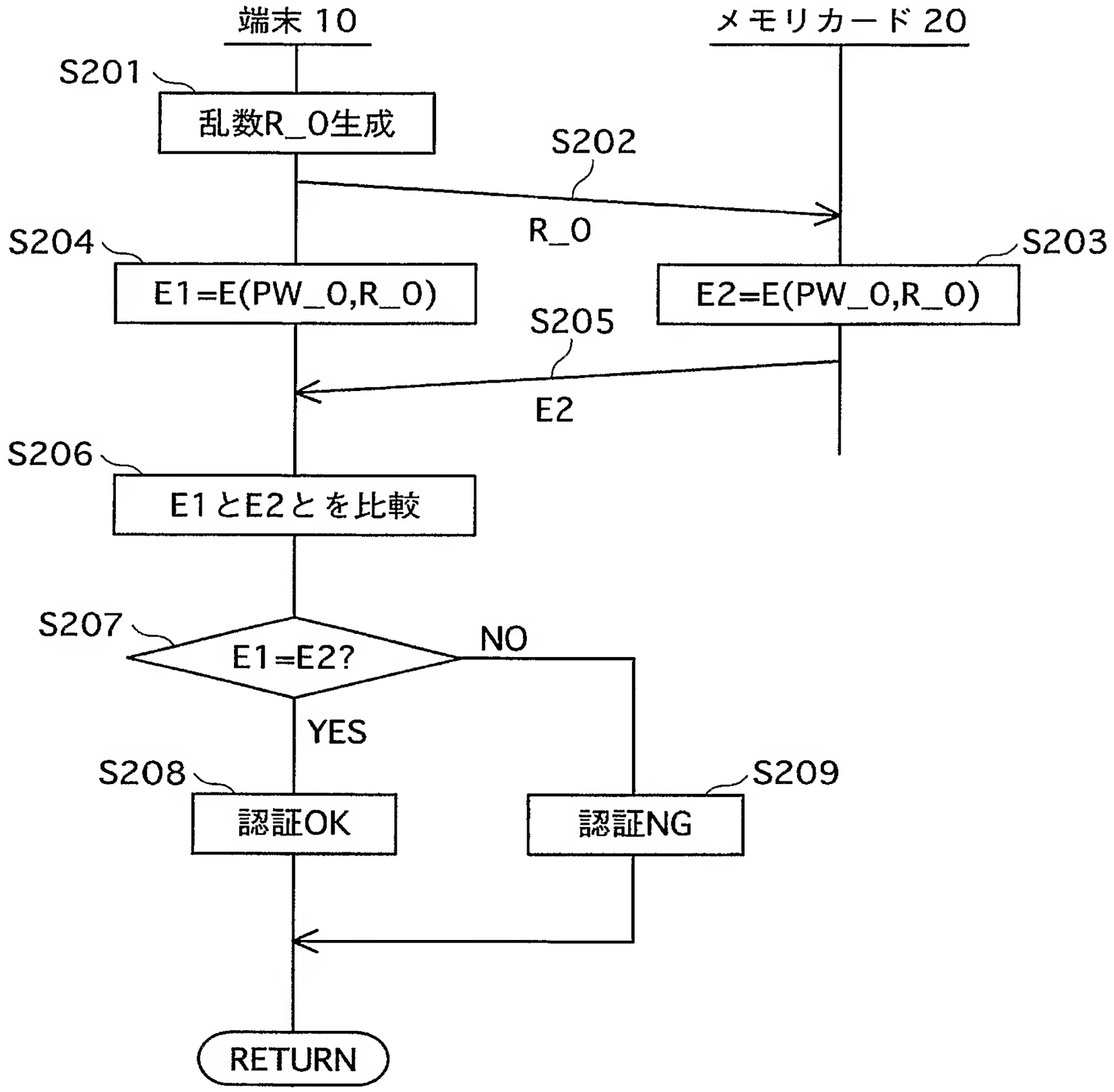
【図５】


30 サーバ装置
304
Cert 管理部
305
登録情報
管理部
306
公開鍵暗号
処理部
302
制御部
303
CRL
格納部
301
通信部
307
コンテンツ
格納部
60

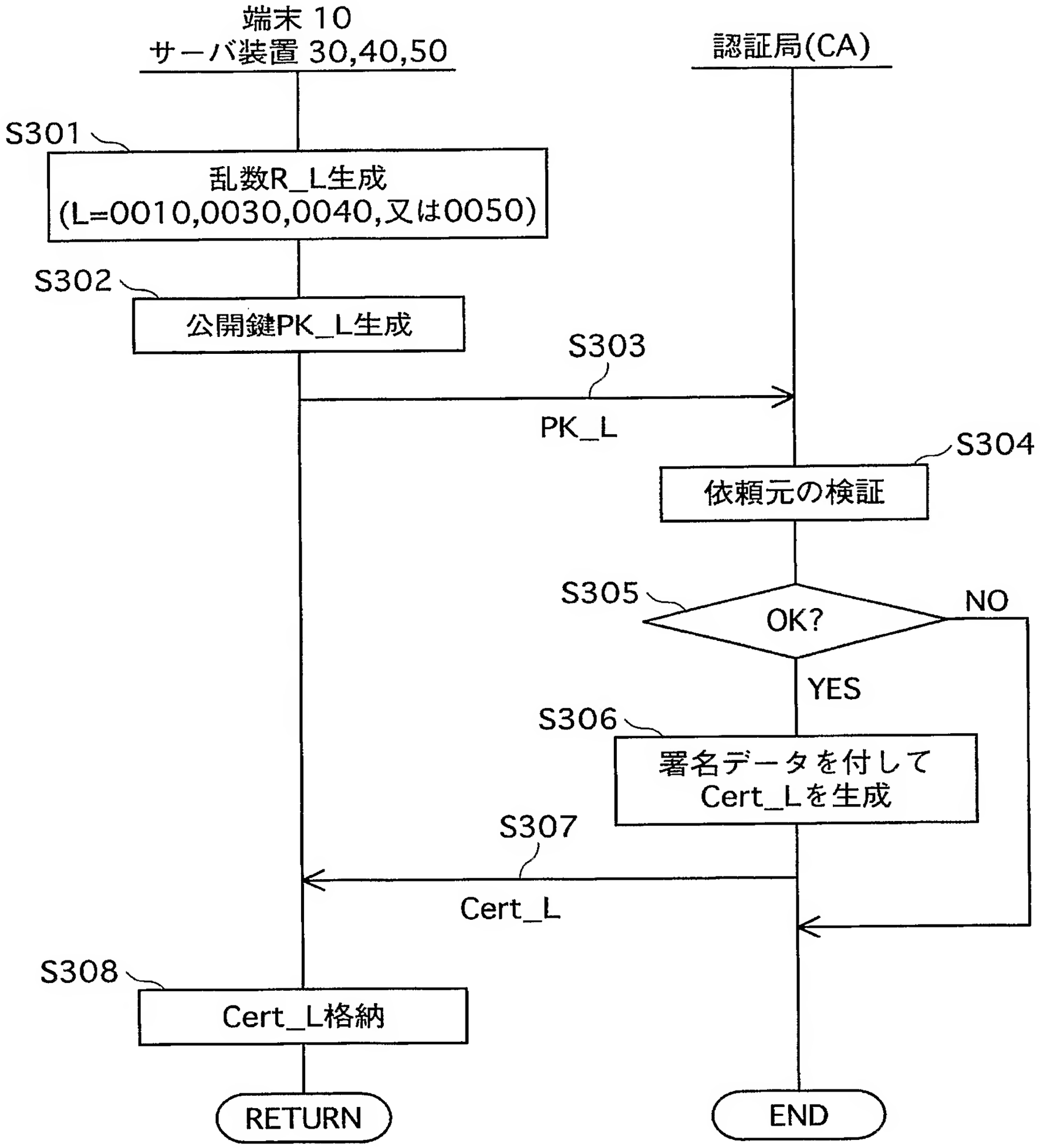
【図６】


端末 10
メモリカード 20
サーバ装置 30
サーバ装置 40
サーバ装置 50
S101
メモリカード20挿入
S102
メモリカード20を認証
S103
OK
NG
END
S104
S105
CAからCert
S106
CAからCert
S107
CAからCert
S108
サービス加入、登録処理
S109
サービス加入、登録処理
S110
サービス加入、登録処理
A
A
A
B

【図７】

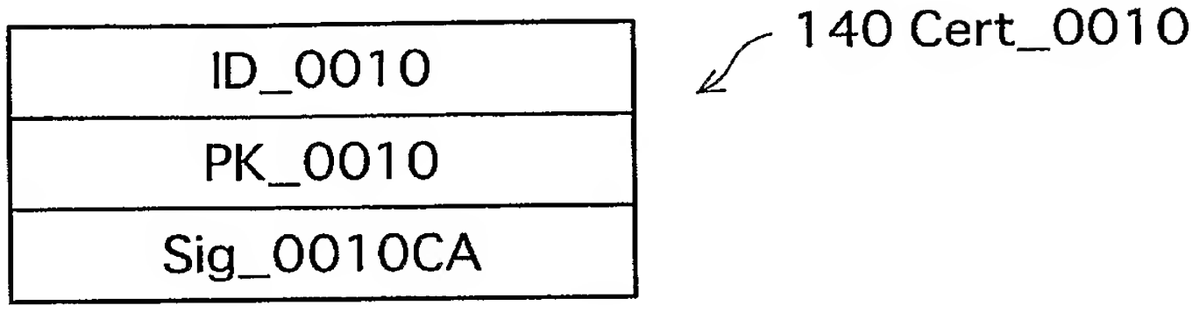

端末 10
メモリカード 20
S201
乱数R_0生成
S202
R_0
S204
E1=E(PW_0,R_0)
S203
E2=E(PW_0,R_0)
S205
E2
S206
E1とE2とを比較
S207
E1=E2?
NO
YES
S208
認証OK
S209
認証NG
RETURN

【図８】

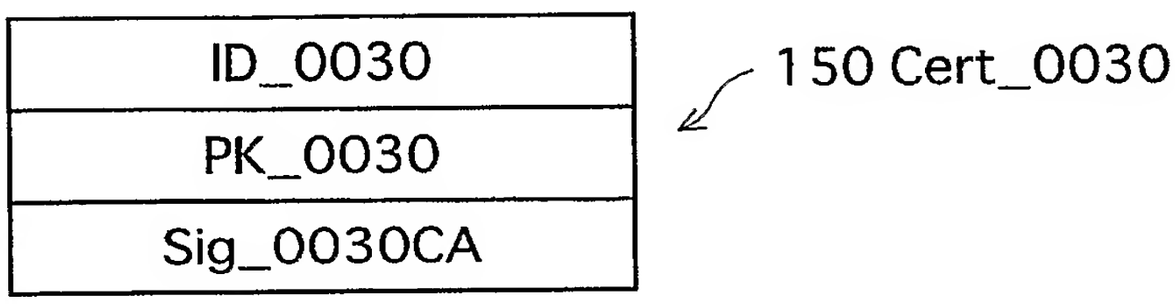

端末 10
サーバ装置 30,40,50
認証局(CA)
S301
乱数R_L生成
(L=0010,0030,0040,又は0050)
S302
公開鍵PK_L生成
S303
PK_L
S304
依頼元の検証
S305
OK?
NO
YES
S306
署名データを付して
Cert_Lを生成
S307
Cert_L
S308
Cert_L格納
RETURN
END

【図９】

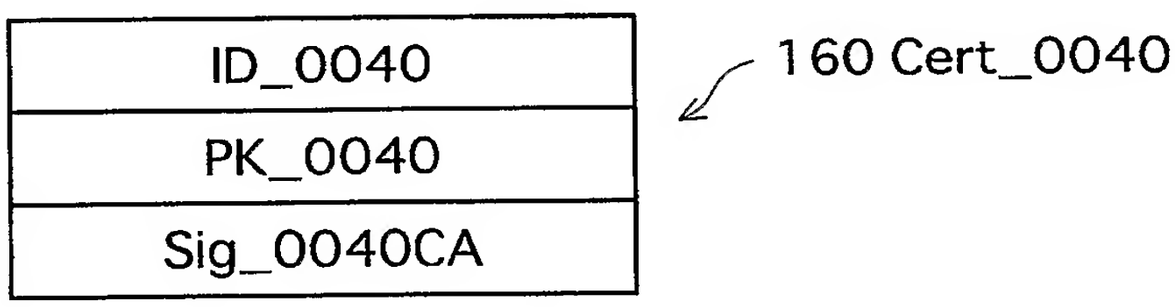
(a) CAから発行される端末 10の公開鍵証明書



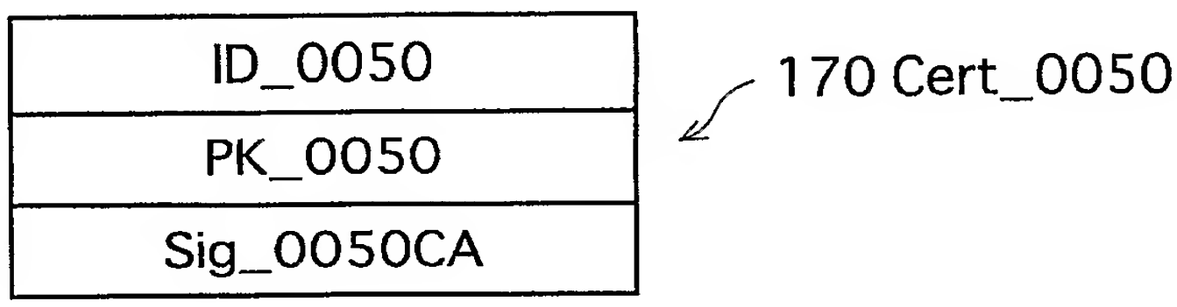
(b) CAから発行されるサーバ装置 30の公開鍵証明書



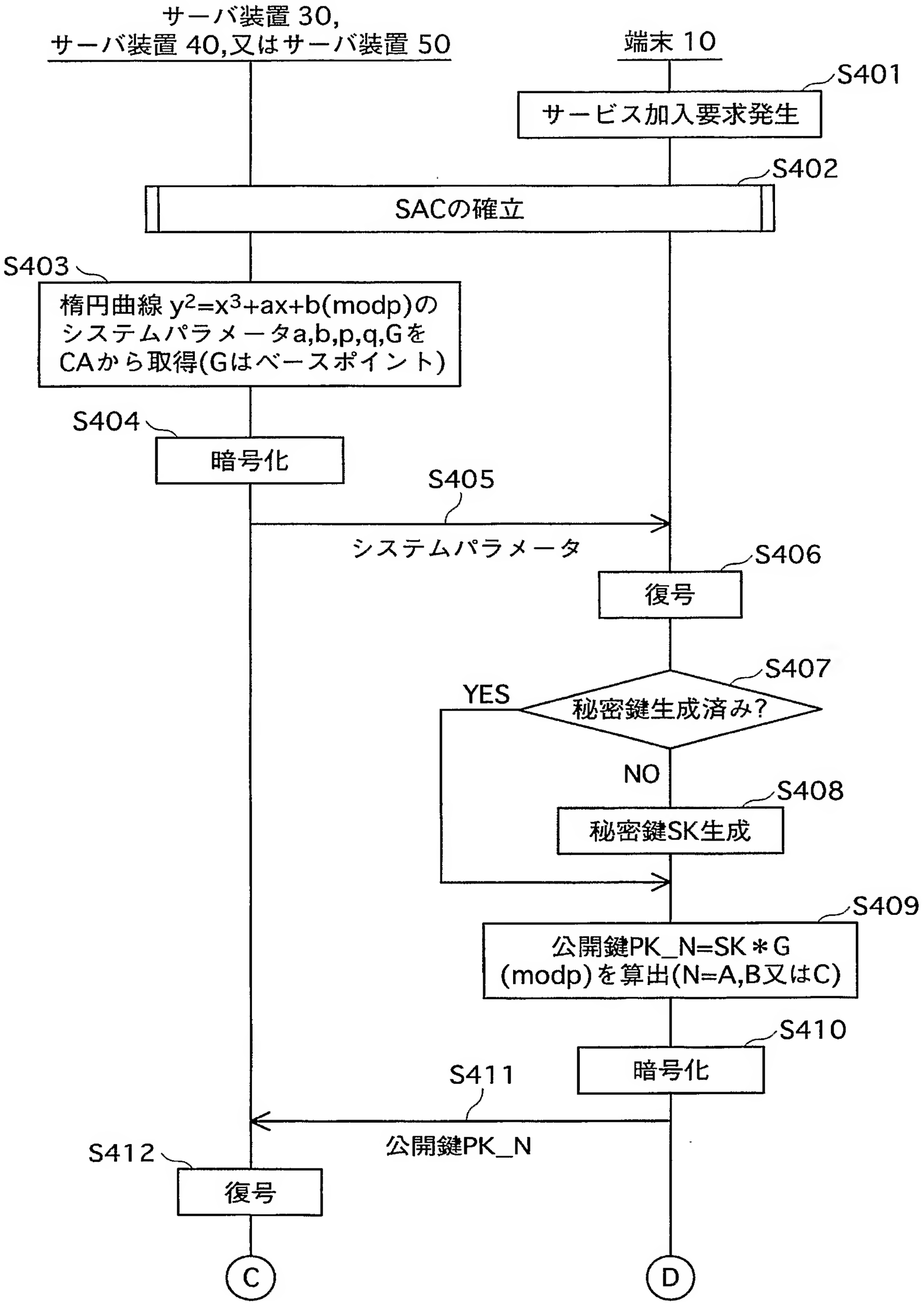
(c) CAから発行されるサーバ装置 40の公開鍵証明書



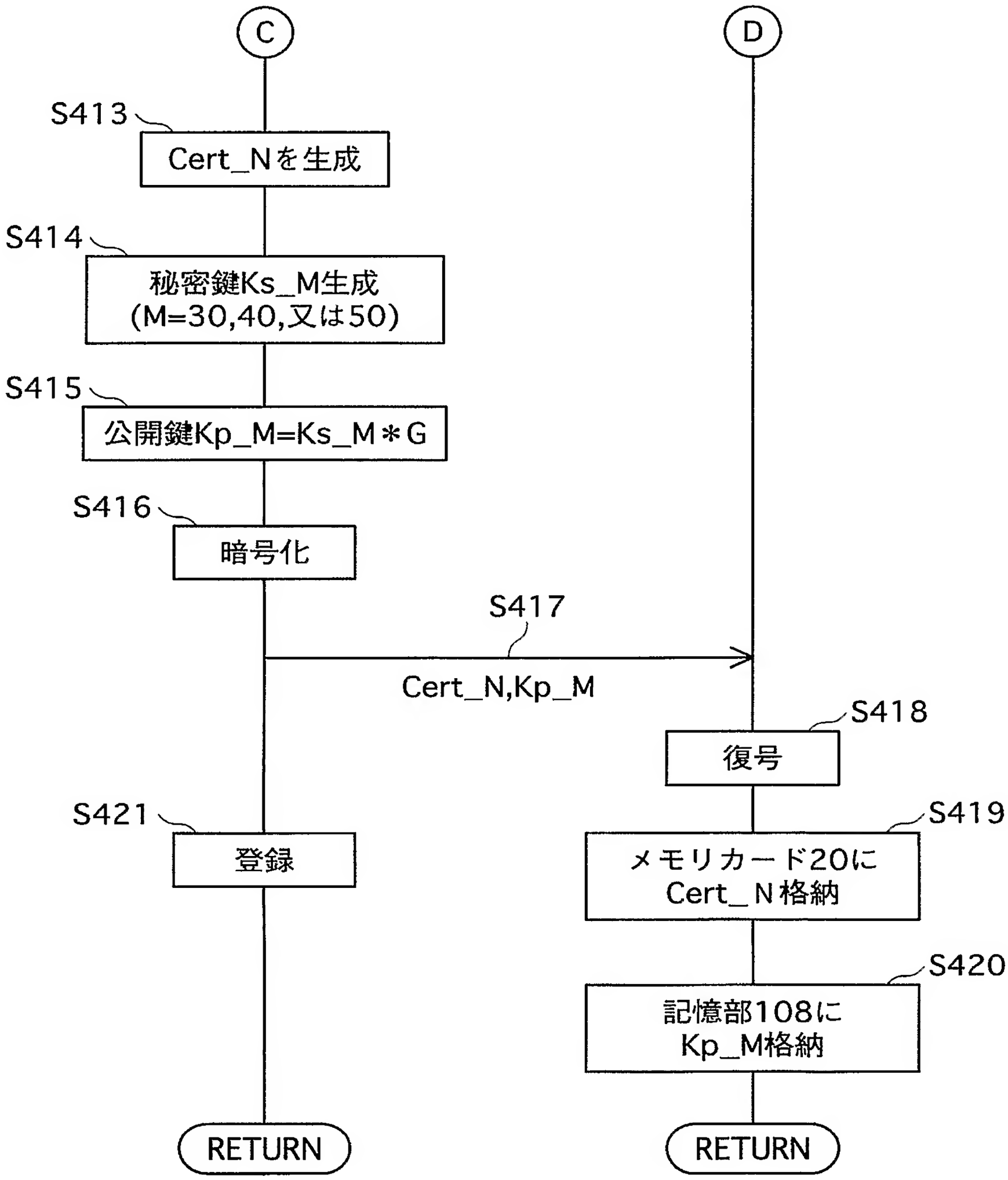
(d) CAから発行されるサーバ装置 50の公開鍵証明書



【図１０】


サーバ装置 30,
サーバ装置 40,又はサーバ装置 50
端末 10
S401
サービス加入要求発生
S402
SACの確立
S403
楕円曲線 y2=x3+ax+b(modp)の
システムパラメータa,b,p,q,Gを
CAから取得(Gはベースポイント)
S404
暗号化
S405
システムパラメータ
S406
復号
S407
YES
秘密鍵生成済み?
NO
S408
秘密鍵SK生成
S409
公開鍵PK_N=SK＊G
(modp)を算出(N=A,B又はC)
S410
暗号化
S411
公開鍵PK_N
S412
復号
C
D

【図１１】


C
S413
Cert_Nを生成
S414
秘密鍵Ks_M生成
(M=30,40,又は50)
S415
公開鍵Kp_M=Ks_M＊G
S416
暗号化
S417
Cert_N,Kp_M
D
S418
復号
S419
メモリカード20に
Cert_N格納
S420
記憶部108に
Kp_M格納
S421
登録
RETURN
RETURN

【図１２】

(a) サーバ装置 30から発行される公開鍵証明書

サービスID	SID_0123A
会員番号	NO_0001
公開鍵	PK_A
署名データ	Sig_A

210 Cert_A

(b) サーバ装置 40から発行される公開鍵証明書

サービスID	SID_0321B
会員番号	NO_0025
公開鍵	PK_B
署名データ	Sig_B

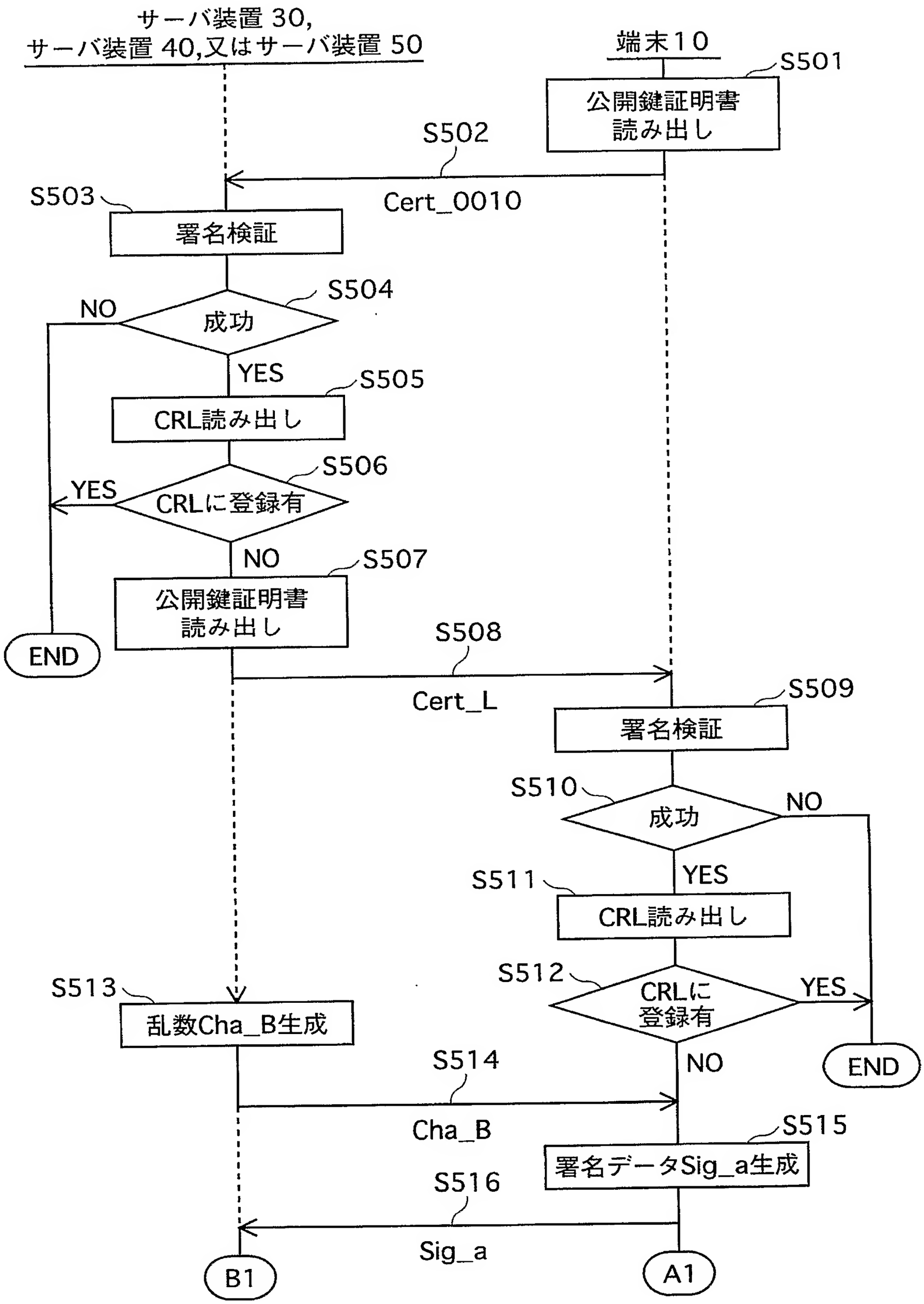
220 Cert_B

(c) サーバ装置 50から発行される公開鍵証明書

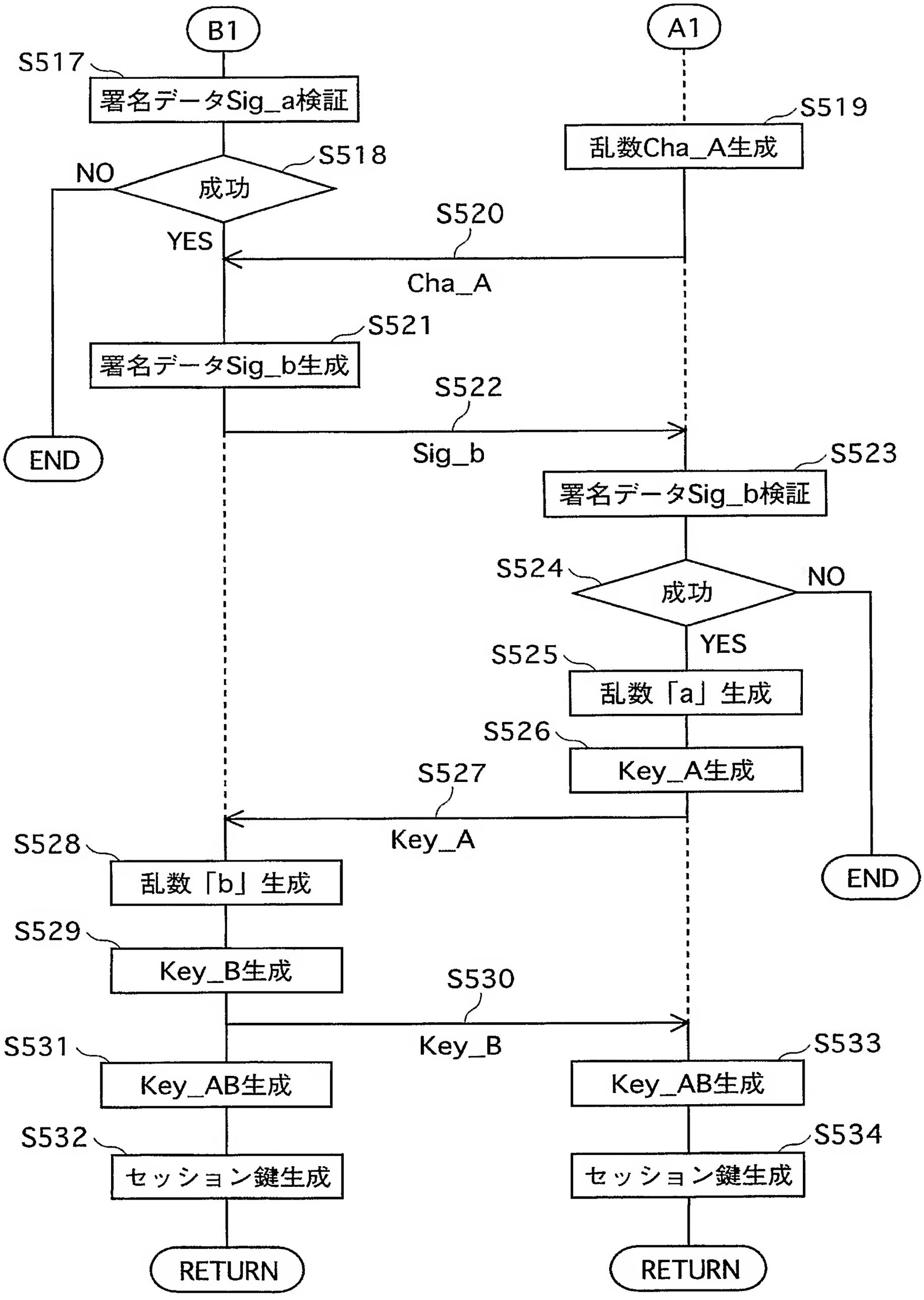
サービスID	SID_0132C
会員番号	NO_3215
公開鍵	PK_C
署名データ	Sig_C

230 Cert_C

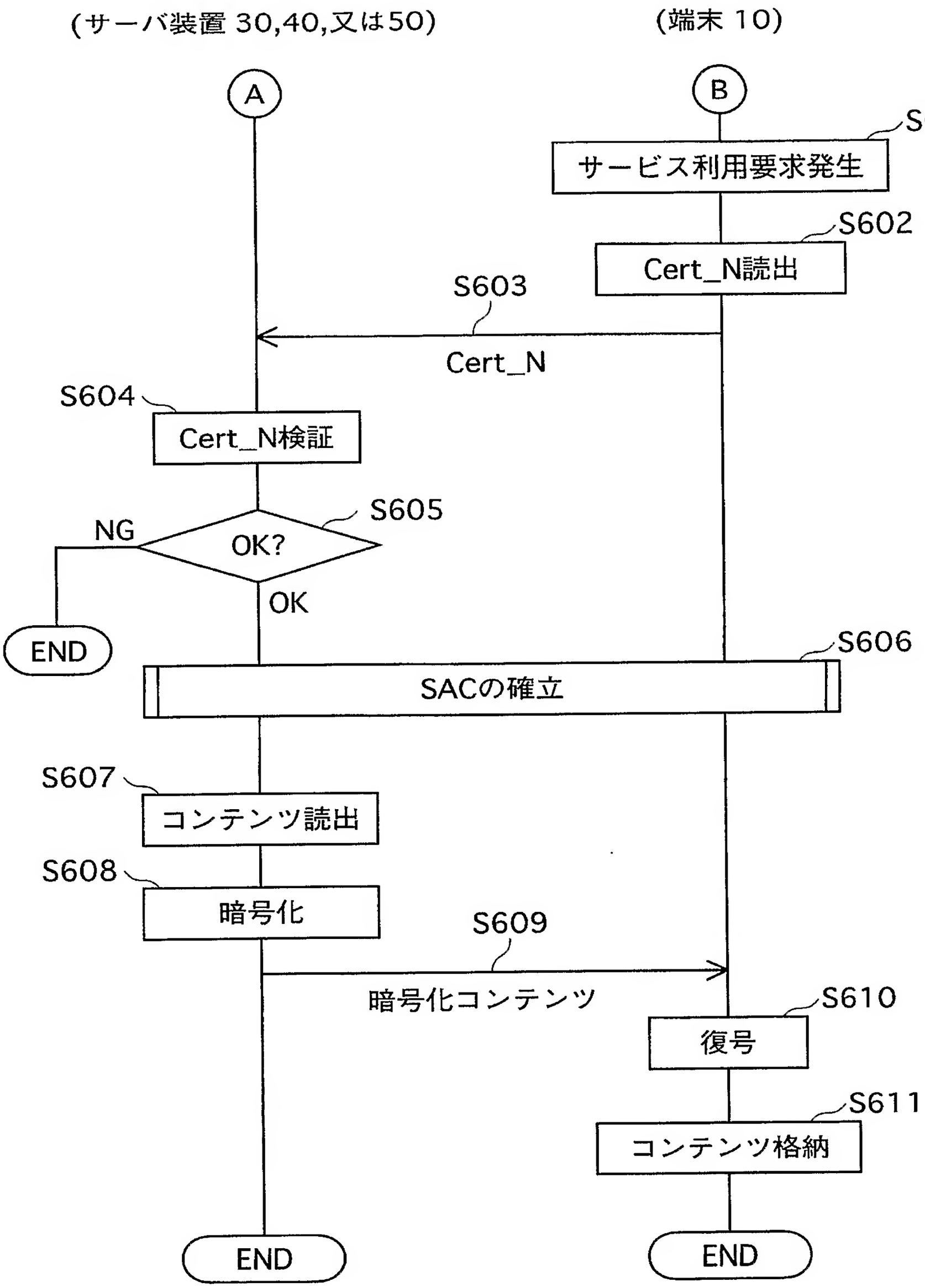
【図１３】


サーバ装置 30,
サーバ装置 40,又はサーバ装置 50
端末10
S501
公開鍵証明書
読み出し
S502
Cert_0010
S503
署名検証
S504
NO
成功
YES
S505
CRL読み出し
S506
YES
CRLに登録有
NO
S507
公開鍵証明書
読み出し
END
S508
Cert_L
S509
署名検証
S510
成功
NO
YES
S511
CRL読み出し
S512
CRLに
登録有
YES
END
S513
乱数Cha_B生成
S514
NO
Cha_B
S515
署名データSig_a生成
S516
Sig_a
B1
A1

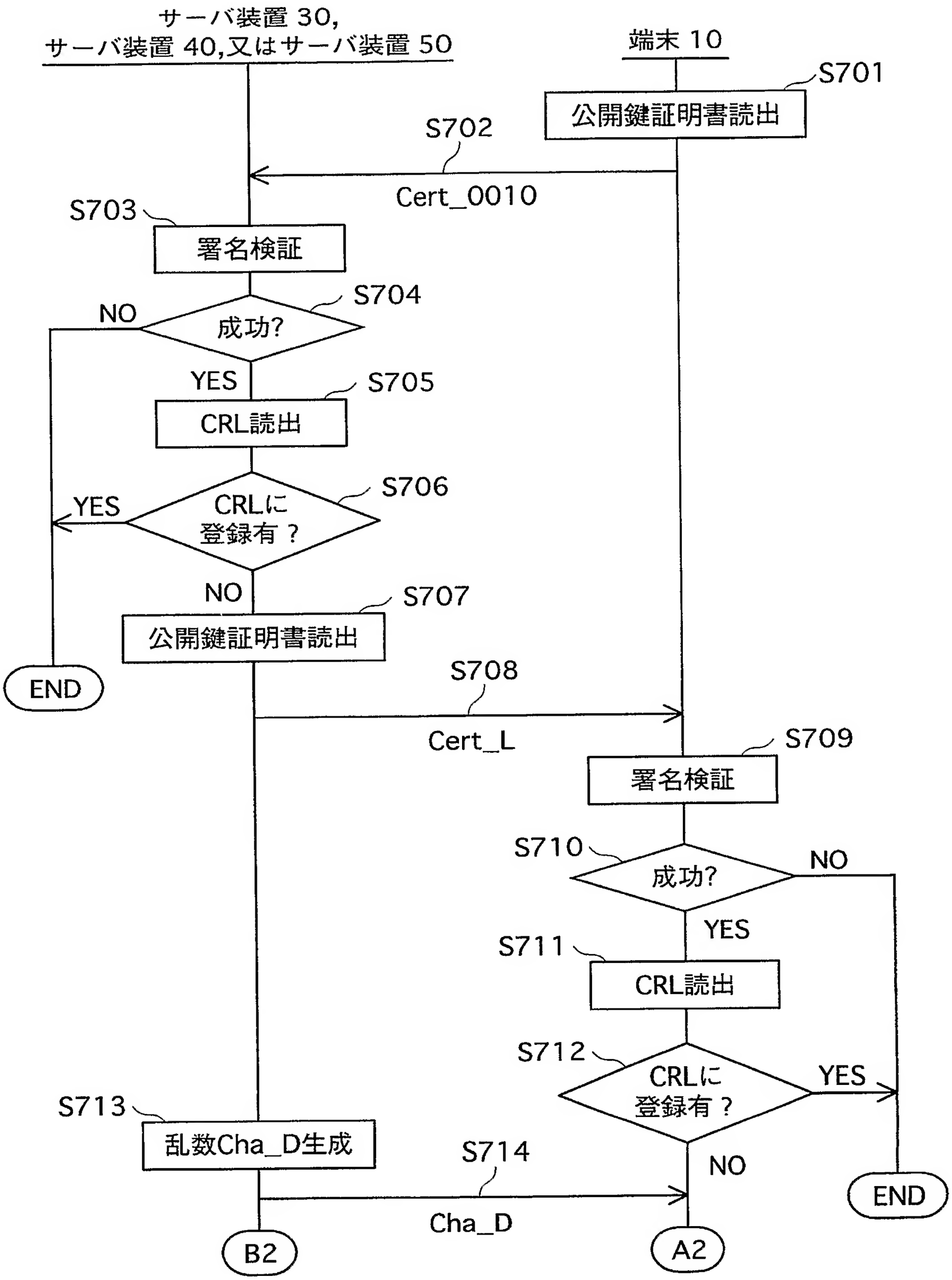
【図１４】


B1
S517
署名データSig_a検証
S518
NO
成功
YES
END
A1
S519
乱数Cha_A生成
S520
Cha_A
S521
署名データSig_b生成
S522
Sig_b
S523
署名データSig_b検証
S524
成功
NO
YES
S525
乱数「a」生成
S526
Key_A生成
S527
Key_A
S528
乱数「b」生成
S529
Key_B生成
S530
Key_B
S531
Key_AB生成
S532
セッション鍵生成
RETURN
S533
Key_AB生成
S534
セッション鍵生成
RETURN
END

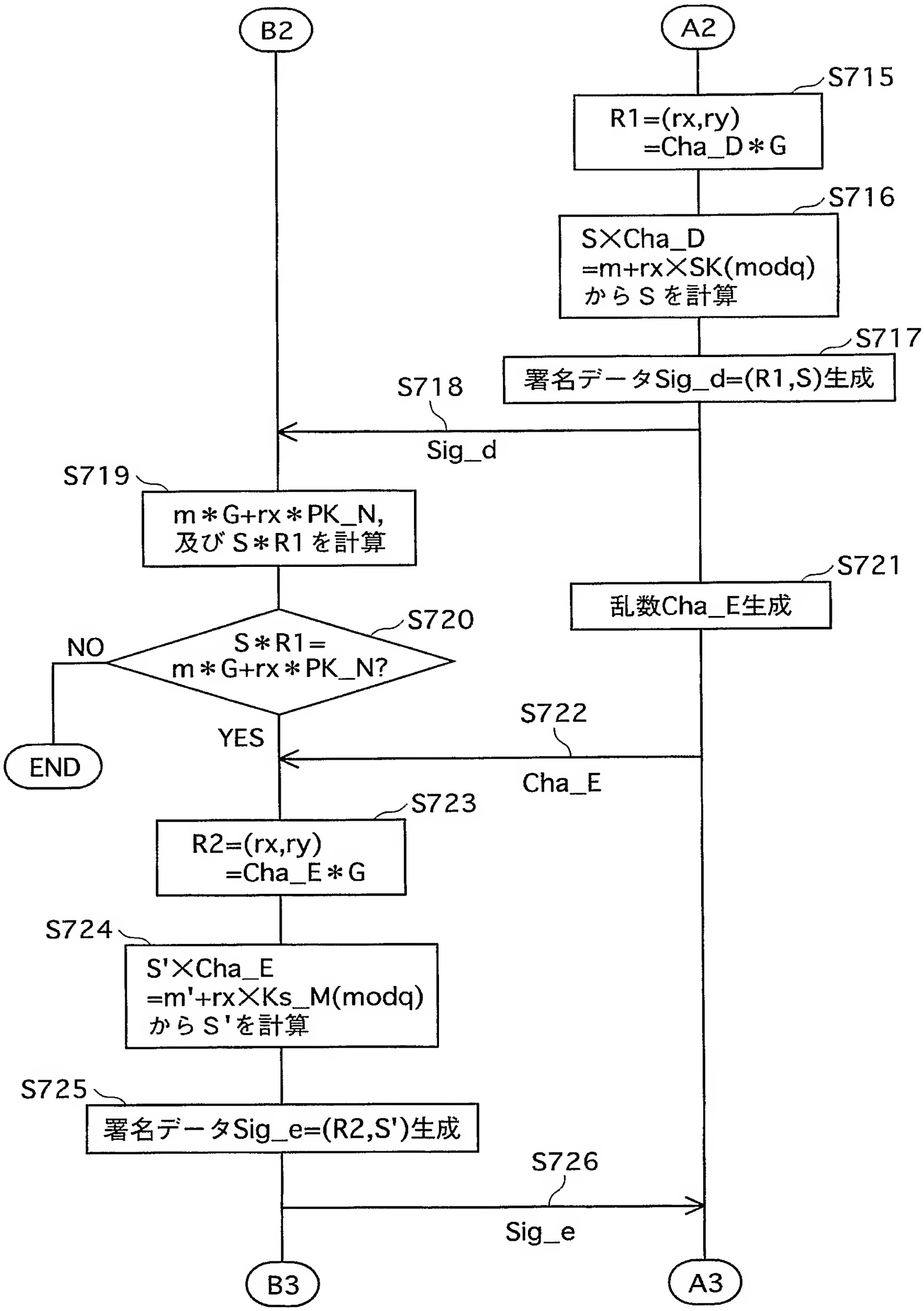
【図１５】


(サーバ装置 30,40,又は50)
(端末 10)
A
B
S601
サービス利用要求発生
S602
Cert_N読出
S603
Cert_N
S604
Cert_N検証
S605
NG
OK?
OK
END
S606
SACの確立
S607
コンテンツ読出
S608
暗号化
S609
暗号化コンテンツ
S610
復号
S611
コンテンツ格納
END
END

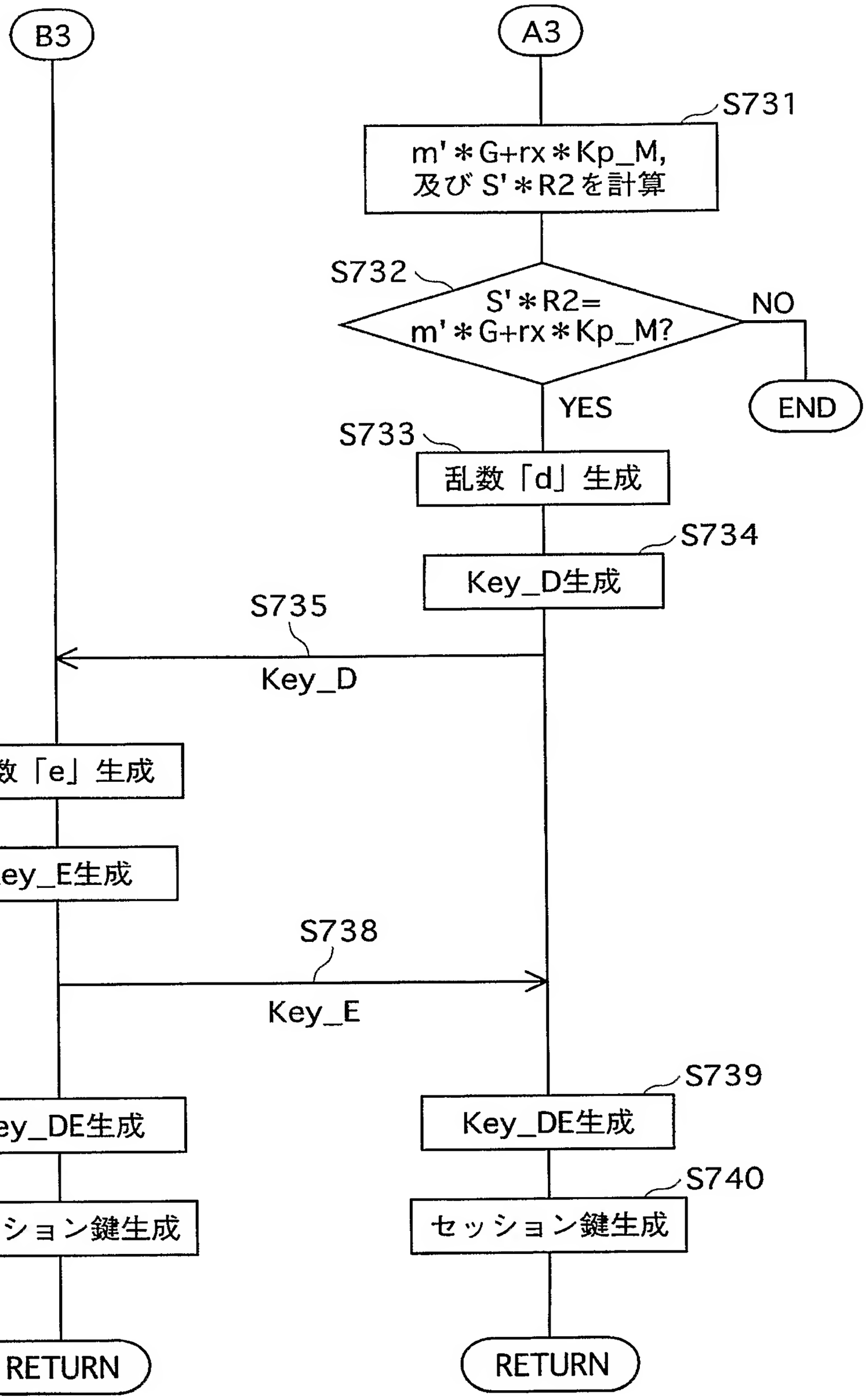
【図１６】


サーバ装置 30,
サーバ装置 40,又はサーバ装置 50
端末 10
S701
公開鍵証明書読出
S702
Cert_0010
S703
署名検証
S704
NO
成功?
YES
S705
CRL読出
S706
YES
CRLに
登録有？
NO
S707
公開鍵証明書読出
END
S708
Cert_L
S709
署名検証
S710
成功?
NO
YES
S711
CRL読出
S712
CRLに
登録有？
YES
NO
END
S713
乱数Cha_D生成
S714
Cha_D
B2
A2

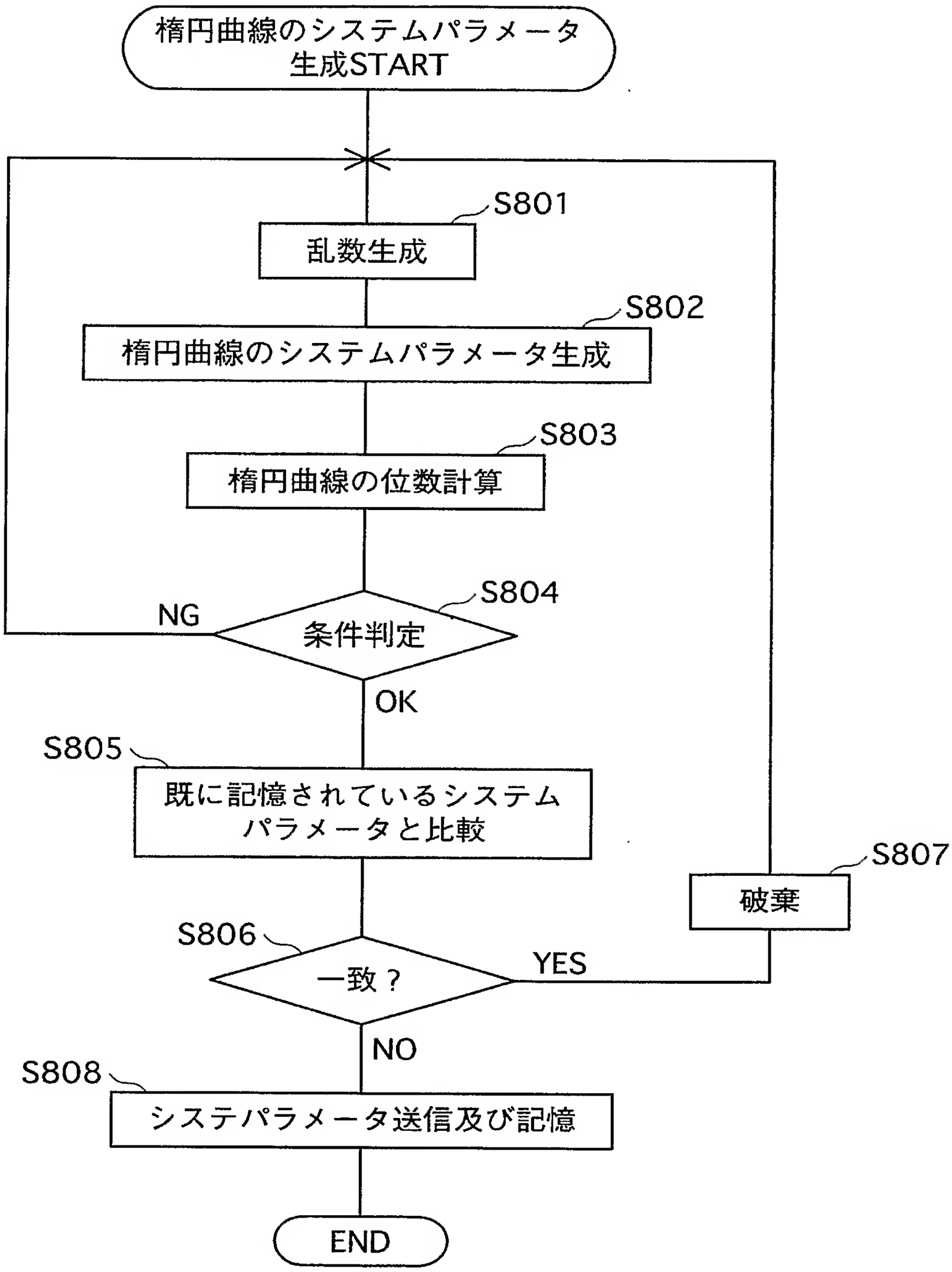
【図１７】


B2
A2
S715
R1=(rx,ry)
=Cha_D＊G
S716
S×Cha_D
=m+rx×SK(modq)
からＳを計算
S717
署名データSig_d=(R1,S)生成
S718
Sig_d
S719
m＊G+rx＊PK_N,
及びＳ＊R1を計算
S721
乱数Cha_E生成
S720
S＊R1=
m＊G+rx＊PK_N?
NO
YES
END
S722
Cha_E
S723
R2=(rx,ry)
=Cha_E＊G
S724
S'×Cha_E
=m'+rx×Ks_M(modq)
からＳ'を計算
S725
署名データSig_e=(R2,S')生成
S726
Sig_e
B3
A3

【図１８】


B3
A3
S731
m'＊G+rx＊Kp_M,
及び S'＊R2を計算
S732
S'＊R2=
m'＊G+rx＊Kp_M?
NO
END
YES
S733
乱数「d」生成
S734
Key_D生成
S735
Key_D
S736
乱数「e」生成
S737
Key_E生成
S738
Key_E
S741
Key_DE生成
S742
セッション鍵生成
RETURN
S739
Key_DE生成
S740
セッション鍵生成
RETURN

【図１９】


楕円曲線のシステムパラメータ
生成START
S801
乱数生成
S802
楕円曲線のシステムパラメータ生成
S803
楕円曲線の位数計算
S804
NG
条件判定
OK
S805
既に記憶されているシステム
パラメータと比較
S807
破棄
S806
一致？
YES
NO
S808
システパラメータ送信及び記憶
END

【書類名】要約書
【要約】
【課題】１台の端末で複数業者のサービスを利用するのに適した情報セキュリティ装置及び情報セキュリティシステムを提供することを目的とする
【解決手段】同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段とを備えることを特徴とする。
【選択図】図１

特願２００４－０７４７３９

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

出証番号　出証特２００５－３０３４１２４